NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

COUNTERMEASURES TO INSIDER CYBER THREATS FOR TURKISH GENERAL COMMAND OF GENDARMERIE

by

Aydın Çini

September 2016

Thesis Advisor:	Shelley P. Gallup
Second Reader:	Thomas Anderson

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704–0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.

1. AGENCY USE ONLY	**2. REPORT DATE** September 2016	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE COUNTERMEASURES TO INSIDER CYBER THREATS FOR TURKISH GENERAL COMMAND OF GENDARMERIE	**5. FUNDING NUMBERS**
6. AUTHOR(S) Aydın Çini	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

Insider threats expose every nation, state, and business entity to danger; however, most of these organizations do not realize this, or they choose to ignore it. Since most studies and technical solutions for insider threats originate from the United States, a good starting point for organizations such as the Turkish General Command of Gendarmerie (TGCG) would be to analyze lessons learned from U.S. examples to try to find ways to adapt countermeasures, considering cultural constraints.

This thesis provides background information about attributes of insider threats, summarizes malicious insiders' characteristics and motivations, and reviews documents (e.g., presidential memorandums, directives, best practices, mitigation strategies) published in the United States for countering insider threats in the United States. Then, technical and non-technical key practices for TGCG are explained. These practices are analyzed in terms of the effects of Turkish culture by using Geert Hofstede's dimensions of national cultures. Finally, recommendations for conceptual implementations of countermeasures to TGCG are presented.

14. SUBJECT TERMS insider, insider threat, cyber threat, transfer of technology, cultural constraints, national cultural dimensions, socio-technical systems, Turkish gendarmerie, Turkish general command of gendarmerie.	**15. NUMBER OF PAGES** 101
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

COUNTERMEASURES TO INSIDER CYBER THREATS FOR TURKISH GENERAL COMMAND OF GENDARMERIE

Aydın Çini
Captain, Turkish Gendarmerie
B.S., Turkish Military Academy, 2003

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 2016

Approved by: Shelley P. Gallup, Ph.D.
Thesis Advisor

Thomas Anderson, Ph.D.
Second Reader

Dan C. Boger, Ph.D.
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Insider threats expose every nation, state, and business entity to danger; however, most of these organizations do not realize this, or they choose to ignore it. Since most studies and technical solutions for insider threats originate from the United States, a good starting point for organizations such as the Turkish General Command of Gendarmerie (TGCG) would be to analyze lessons learned from U.S. examples to try to find ways to adapt countermeasures, considering cultural constraints.

This thesis provides background information about attributes of insider threats, summarizes malicious insiders' characteristics and motivations, and reviews documents (e.g., presidential memorandums, directives, best practices, mitigation strategies) published in the United States for countering insider threats in the United States. Then, technical and non-technical key practices for TGCG are explained. These practices are analyzed in terms of the effects of Turkish culture by using Geert Hofstede's dimensions of national cultures. Finally, recommendations for conceptual implementations of countermeasures to TGCG are presented.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

CERT	Computer Emergency Response Team
CI	counterintelligence
DITMAC	DOD Insider Threat Management and Analysis Center
DLP	data loss prevention
DOD	Department of Defense
DON	Department of Navy
InT	insider threats
INV	individualism index
IT	information technology
ITTF	Insider Threat Task Force
ITPM	Insider Threat Prediction Model
ITPT	Insider Threat Prediction Tool
LE	law enforcement
MAS	masculinity index
NITTF	National ITTF
PDI	power distance index
SIEM	Security Information and Event Management
SIFMA	Securities Industry and Financial Markets Association
STS	socio-technical system
TGCG	Turkish General Command of Gendarmerie
TOT	transfer of technology
UAI	uncertainty avoidance index
UAM	user activity monitoring
UIT	unintentional insider threat
U.S.	United States

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

First of all, I want to thank to my wife, Buket, and my son, Ege İbrahim. I cannot imagine any success in my life without your love and support. Thank you for being so patient with me. I love you both.

I appreciate the contributions of Dr. Shelley Gallup and Dr. Thomas Anderson as my thesis advisors. Sirs, with your guidance and help I was able to keep my work on the right track. I also want to thank SL Glenn Cook for his contribution to my knowledge, and for being a great Academic Associate.

Lastly, I want to thank the Turkish General Command of Gendarmerie for giving me the opportunity of studying at the Naval Postgraduate School. In addition to great knowledge, I collected great memories.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Is your organization protected against someone who knows your system better than anyone else? This is an important question for anticipating insider threats (InT). The concept of InT is not new. However, advances in technology have added complexity to this area. Big organizations have become heavily dependent on information systems for managing data and information critical to operations and maintaining domain advantage. This poses a clear and present threat, as malicious users can exploit vulnerabilities that exist inherently within information systems to steal information secrets or sabotage systems.

To illustrate, Chelsea Manning, a United States (U.S.) Army soldier, leaked more than 750.000 documents, including military and diplomatic secrets (Tate, 2013). Similarly, Edward J. Snowden, a computer professional and former U.S. Central Intelligence Agency and government worker, also leaked information from the U.S. National Security Agency and United Kingdom government in 2013 (Dedman, Brunker, & Cole, 2014). These are very well-known examples, but outside of the U.S., breaches often remain unreported and are kept inside the organizations.

Even when insider incidents are publicized and law enforcement units are involved, they are not necessarily recorded in a database for future research and analysis. As an important exception, Carnegie Mellon University Computer Emergency Response Team (CERT) Division has kept over 700 cases in its InT database in more than 15 years and may have the most comprehensive data about U.S. insider incidents. The InT database and analyses of insider incidents by the CERT Division are important contributors to studies about mitigating InT in U.S. organizations, both public and private.

Considering the given insider incidents, InT issues now hold an important place in U.S. national security policy. For example, the Presidential Memorandum (Obama, 2012) for national InT policy states that InT must be considered as a significant threat to national security, and all organizations must implement actual countermeasures against insiders who want to do harm to organizations or people. Consequently, the efforts to mitigate InT risks in U.S. organizations have led to the emergence of technical and non-technical InT countermeasures.

A. PROBLEM

Insiders expose every country or organization to danger. However, most of the organizations do not realize this, or they choose to ignore it. Without InT risk mitigation capabilities they are vulnerable to insider attacks that may cause damage to internal networks, databases, and sensitive data.

For this thesis, the problem is that Turkish General Command of Gendarmerie (TGCG) has few mitigation capabilities, such as policies, defined countermeasures (technical or non-technical), and a designated organizational unit (such as an InT analysis hub), to prevent and protect against the insider cyber threats.

B. PURPOSE

Upon acknowledgement of the importance of the insider threat problem, it is vital to take action against InT before it is too late. Instead of starting from scratch, a good starting point for the TGCG organization would be to analyze lessons learned from similar examples and try to find ways to adapt countermeasures while considering cultural constraints.

Thus, the purpose of this thesis is to analyze U.S. InT policies, procedures, countermeasures, and organizational structures and adapt what is learned to the TGCG. Adaptation of this capability from the U.S. to Turkey implies cross-cultural aspects that will also need to be understood and a framework for analysis defined in order to be successful.

C. HYPOTHESES AND RESEARCH QUESTIONS

As the starting point, the first hypothesis of this thesis is that given that the indicators for insider cyber threats are nearly the same between cultures, with some nuances, counter insider cyber threat policies, technologies, and organizations should be transferrable between different countries. Following this hypothesis, the second focuses on the differences of national cultures that may affect transfer of counter-InT technology. Thus, second hypothesis claims that even though there are cultural differences between countries, these adapted countermeasures should stay effective, and thus may be a robust transference of knowledge and capability pertaining to InT mitigation between cooperating countries.

The two questions to be answered in this thesis are as follows:

Q1. What are the countermeasures, both technical and non-technical, and organizational structures that can be adapted from U.S. examples to TGCG?

Q2. What are the cultural constraints for TGCG that pertain to the effectiveness of InT technology transfer?

D. RESEARCH METHOD

Implementation of InT risk mitigation capability to another country is, in fact, a transfer of technology that includes people, processes, and products. Since the two sides of this transfer include interacting individuals and information systems, socio-technical systems theory becomes important for this thesis.

Based on socio-technical systems theory, the mitigation strategies and best practices that are derived from scholarly works, technical reports (e.g., CERT publications), guiding documents (e.g., the Presidential Memorandum on InT), and industry recommendations (e.g., SIFMA InT Best Practices Guide) will be divided into two parts: Non-technical countermeasures, which are related to the social subsystem, and technical countermeasures, which are related to technical subsystem.

According to Kedia and Bhagat’s (1988) approach, there exist cultural constraints on technology transfer, and societal culture-based differences have moderating effects on this transfer. Thus, in order to understand cultural constraints on transferring InT technology to TGCG, strategies and countermeasures are analyzed using Geert Hofstede’s national cultures framework.

Since culture plays a more important role in the social subsystem, five non-technical countermeasures are analyzed individually and four technical countermeasures are analyzed as a whole. Based on the analysis results, recommendations for minimizing cultural constraints on transferring counter InT capability to TGCG are provided in the last chapter.

E. ORGANIZATION OF THE THESIS

Chapter II reviews literature on insiders and InT that include attributions, motives, characteristics, and psychosocial indicators of insiders and InT prediction models.

Chapter III explains and establishes links between the socio-technical systems theory, transfer of technology approach, and national cultural dimensions.

Chapter IV and Chapter V present non-technical and technical countermeasures to prevent and respond to InT and the effects of these countermeasures on Turkish culture.

Chapter VI presents recommendations to TGCG for minimizing cultural differences while implementing counter InT capabilities and proposes an InT hub structure, makes suggestions for future work, and concludes the thesis.

II. THE PROBLEM OF INSIDER THREATS

InT has become an important problem for organizational computer systems as the utilization of technology and information systems in organizations has grown over time. In fact, InT is now known as "one of the most serious security problems" to deal with because of the advantageous position of insiders (Hunker & Probst, 2011, p. 4). As the InT problem has received great attention, the number of studies about insiders has also increased considerably.

These studies include relevant definitions, prevention and detection techniques, policies, countermeasures, and best practices to better understand the InT problem and develop effective ways to mitigate that threat. Most of the studies have come out since 1999 when RAND Corporation started a series of workshops to provide insight into the problem and the U.S. Department of Defense (DOD) released its own report on policy changes and research directions (Hunker & Probst, 2011). Based on those studies, this chapter attempts to understand the InT problem as much as possible in all of its aspects.

A. DEFINITION OF INSIDER AND INSIDER THREAT

Since the InT research deals with some of the most challenging issues in information security, providing uniform definitions of "insider" and "insider threat" has proven difficult (Costa et al., 2014). This is because there have been discussions about InT that have resulted in "numerous models and frameworks," each of which has a different perspective on the problem (Nurse et al., 2014). However context-dependent they might be, it is essential to provide definitions for reliable identification and mitigation of InT.

Before defining the InT, it is important to understand who is an insider. One can find different definitions of insider in varying resources. For example, a common one is provided by the U.S. Department of Homeland Security in a research project on InT. Here "an insider is defined as an individual with privileged access to an IT system" (Hunker & Probst, 2011, p. 5).

This definition, like other various definitions, seems specific enough to some degree, but rapid development in technology and IT systems is continuously changing the boundaries of this definition. Especially, ubiquitous networked IT capabilities and loose boundaries between the inside and outside of the organizations require a broader definition (Hunker & Probst, 2011).

Probst, Hunker, Gollmann, and Bishop (2008) provide a broader, trust-based definition such as "an insider is a person that has been legitimately empowered with the right to access, represent, or decide about one or more assets of the organization's structure" (p. 5). Probst and his colleagues believe that this definition does not include any IT bias.

The definitions of InT and the insider are closely related. Similarly, insider studies provide and emphasize several main factors, such as the nature of misuse, maliciousness, an intentional vs. unintentional act, visibility of event, insider's skill, and motivation as determinants of the InT. Hunker and Probst (2011) provide a detailed overview on InT, and they state, "If one cannot precisely define the problem, how can one expect to address it?" (p. 7).

In most of the studies, the terms insider and InT share the same meaning and purpose. Scholars focus on different aspects of the problem rather than providing a clear distinction of insiders and InT. Maybe the problem is that there exist many different types of insider and it is not easy to distinguish determinants of the InT in advance.

Yet, there exists a common definition of InT that combines the threat and the individual who poses that threat. It is provided by Cappelli, Moore, and Trzeciak and we use this definition to define insiders.

> A malicious insider threat is as a current or former employee, contractor, or business partner who has or had authorized access to an organization's network, system, or data and has intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems. (Cappelli, Moore, & Trzeciak, 2012, p. xx)

This definition excludes unintentional InT (UIT), which is an important part of InT. The Carnegie Mellon University CERT researchers define UIT by slightly modifying the malicious InT definition to include “system, or data and who, through action or inaction without malicious intent, causes harm or substantially increases the probability of future serious harm to confidentiality” (Cappelli et al., 2012, p. 357).

Although recognizing the importance of UIT, this study primarily focuses on the malicious insiders based on two reasons. Firstly, the literature on UIT is very limited because organizations are prone to handle UIT issues internally since they are not illegal or criminal. Secondly, as Cappelli et al. state (2012), most of the countermeasures against malicious insiders can also be effective against UIT.

After defining malicious and unintentional InT, we must state that malicious InT vary with respect to types of crimes committed (Cappelli et al., 2012). The CERT team, which keeps an InT database that includes more than 700 cases and work on InT over ten years, identifies four types of crimes: “IT sabotage,” “espionage,” “theft of intellectual property,” and “fraud.” The definitions of three of these are as follows:

> IT sabotage: An insider’s use of information technology (IT) to direct specific harm at an organization or an individual.
>
> Theft of intellectual property (IP): An insider’s use of IT to steal intellectual property from the organization. This category includes industrial espionage involving insiders.
>
> Fraud: An insider’s use of IT for unauthorized modification, addition, or deletion of an organization’s data (not programs or systems) for personal gain, or theft of information that leads to an identity crime (e.g., identity theft, credit card fraud). (Cappelli et al., 2012, p. xxi)

Cappelli and her colleagues also provide a national security espionage definition, and they state that since they work in the area of espionage, the findings are available for a limited audience. However, this limitation does not have major implications for this thesis because “IT sabotage” and “espionage” are not very different crime types. They are “variations on the same aberrant behavior” (Band et al., 2006, p. 7). This means identical or similar technical and non-technical countermeasures might be used to detect and deter insider espionage crimes.

Identifying the problem is the first step to solving it. Another important step is to understand the insider. In order to deter, predict, prevent, and detect the insider, it is crucial to understand the characteristics, attributes, motives, and psychology of the insider.

B. ATTRIBUTES OF THE INSIDER

Wood (2000) provides some foundational assertions and assumptions to propose a model for simulating malicious InT. Wood (2000) states that a malicious insider can be described from a variety of attributes, which are briefly presented as follows:

Access: The insider can access the system or some part of the system without being checked or arousing suspicion. An outside attacker who can penetrate the system is not considered as an insider unless he or she has other attributes of the insider.

Knowledge: The insider has good knowledge of the system and has detailed information on the target. In some cases, the insider is the only one who is an expert on the target.

Privileges: The insider should have enough privileges to launch an attack to the target. The insider does not need to have root or administrator access to the system. It is enough to recruit someone who has privileges to mount an attack.

Skills: The insider has enough skill to mount an attack to the system. As an assumption, the insider may actually be a local domain expert and it is unlikely for him/her to attack unfamiliar parts of the system.

Risk: The insider usually avoids risk. A worst-case scenario for an insider can be the disclosure of his plan before mounting the attack. To minimize the risk, the insider generally works alone.

Tactics: Depending on the aims of the attack, the tactics of the insider change completely. Some basic attack tactics are plan-run-hit, attack and run, attack until caught, and espionage.

Motivation: The insider mounts an attack on target system to achieve some of the following goals: To make a profit, to provoke change on the system, to subvert the mission of the organization, to satisfy a personal motive such as revenge.

Process: Wood provides some basic steps for an insider attack that are “someone becomes motivated to attack,” “adversary identifies the target,” “adversary plans operation,” and “launch attack.”

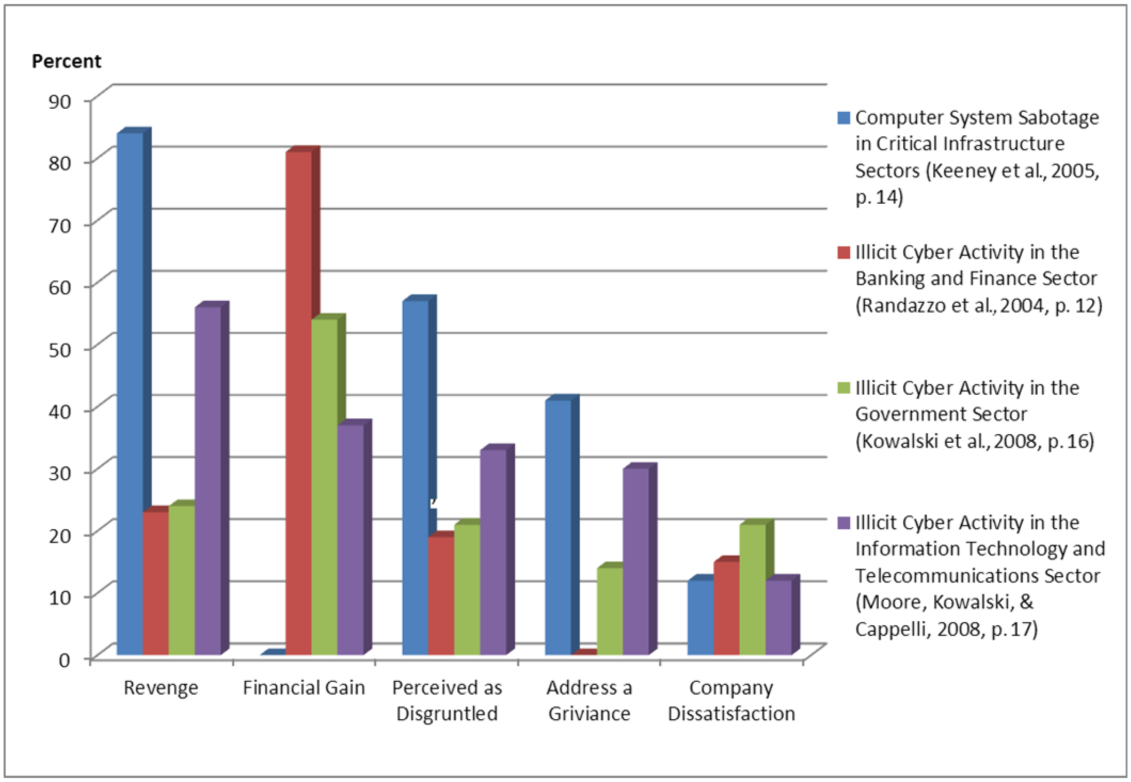
C. MOTIVES OF THE INSIDER

The motives of the insider represent an important part for understanding the problem. Beginning with the study of Randazzo, Keeney, Kowalski, Cappelli, and Moore (2004), CERT researchers provided the motives of insiders within different sectors. Figure 1 is derived from four different studies and it represents the major insider motivations for different sectors.

According to findings, money is the primary motivation factor for the insiders working in banking, finance, and government sectors. Revenge appears to be the main reason for insider attacks in critical infrastructure, information technology, and telecommunication sectors. For all the sectors examined, some insiders were also perceived as disgruntled, and they were not actually satisfied with their companies’ policies or cultures.

Other motivations of the insiders that are not depicted in Figure 1 are garnering respect (critical infrastructure, banking, and finance sectors) and taking information to new employer (IT and telecommunication sectors). Total percentages for each sector exceed 100 percent because insiders had more than one motivation for their attacks (Keeney et al., 2005).

According to Cappelli et al. (2012), disgruntlement of an insider due to unmet expectations is pervasive among IT sabotage cases. Insiders’ level of expectation increases on some specific factors based on the time spent in the organization. Usually a precipitating event leads to unmet expectations that trigger disgruntlement (Cappelli et al., 2012).



Adapted from Keeney et al. (2005); Randazzo et al. (2004); Kowalski et al. (2008); Moore, Kowalski, & Cappelli et al. (2008).

Figure 1. Major Motivations of the Insiders for Different Sectors.

An unmet expectation can be defined as "an unsatisfied assumption by an individual that an organization action or event will (or will not) happen, or a condition will (or will not) exist" (Cappelli et al., 2012, p. 357). Cappelli and her colleagues (2012) provide some examples of unmet expectations from insider cases. Those include

- Salary /bonus
- Promotion
- Freedom of online actions
- Project requirements
- Use of company resources (Cappelli et al., 2012, p. 33)

Cappelli et al. (2012) define a precipitating event as something that limits or "terminates the freedom of recognition to which the insider has been accustomed to" do/have (p. 32). Those events include

- Promotion denial
- Demotion due to project completion
- Transfer between departments
- Access changed
- Financial
- Disagreement over salary and compensation
- Bonuses lower than expected (Cappelli et al., 2012, p. 33)

D. CHARACTERISTICS OF THE INSIDER (PERSONAL PREDISPOSITIONS)

Band et al. (2006) examine the factors that contribute to the insiders' betrayal of trust (for IT sabotage and espionage), and they state understanding that the insiders' psychosocial motivations gives "insight into some security vulnerabilities and future investigative strategies" (p. 1). From their study, the first observation for two types of insiders is that "most saboteurs and spies had common personal predispositions that contributed to their risk of committing malicious acts" (Band et al., 2006, p. 13). Here, the personal predispositions represent the individual-level characteristics that can contribute to the risk of being an InT (Band et al., 2006).

Band and his colleagues group "personal predispositions" into four categories, which are "serious mental health disorders," "personality problems," "social skills and decision-making deficits," and "history of rule violations." The brief explanations of each category can be as follows.

"*The mental health disorders* category" threatens the "insiders' ability to function successfully in their job and in personal relationships at work" (Band et al., 2006, p. 73). Some observables for this category include

> Addiction or behaviors that impair professional abilities resulting in intervention or sanction; psychiatric medications that are being taken; psychological treatment is recommended or administered; insider complains to others of psychological symptoms, symptoms are noticeable by peers (absenteeism, mood, concentration problems); legal problems

> related to disorder (driving while intoxicated, arrests, debt). (Band et al., 2006, p. 76)

Personality problems include "self-esteem deficits and patterns of biased perceptions of self and others that impact personal and professional decision making in consistently maladaptive ways for the individual" (Band et al., 2006, p. 73). Example observables for personality problems include

> Unusual needs for attention, sense of entitlement such that he is above the rules, chronic dissatisfaction with aspects of job or personal feedback, forms grudges, feels unappreciated, unrealistic expectations of others, arrogance, personal conflicts, fearful of usually routine experiences, compensatory behaviors designed to enhance self-esteem (spending, bragging, bullying). May or may not manifest in flagrant social skills problems (vs. withdrawal). (Band et al., 2006, p. 76)

"Social skills and decision-making deficits" refer to "chronic problems getting along and working with others, due to active social tension or conflict attributable to the insider or active withdrawal from contact on the insider's part" (Band et al., 2006, p. 75). Some of the observables derived from cases that were examined by Band and his colleagues include

> Isolation from the group, propensity for interpersonal conflicts with supervisors, lack of expected professional advancement, frequent transfers, avoidance by peers, stereotyping (geek, loser, weird), scapegoating/bullying, misinterpretation of social cues. With lack of impulse control and/or conscience, chronic rule violations as in sociopathy. (Band et al., 2006, p. 77)

The final category of personal predispositions concerns the insiders who have a "*record of breaking rules* ranging from prosecuted legal violations and convictions to violations of security regulations to participation in financial conflicts of interest" (Band et al., 2006, p. 75). The observables for this category range from "arrests, hacking, security violations, harassment or conflicts resulting in official sanctions or complaints, misuse of travel, time, and expenses (Band et al., 2006, p. 77).

E. PREDICTING INSIDER ATTACKS

According to Schultz (2002), insider attacks are "the intentional misuse of computer systems by users who are authorized to access those systems and networks." He said that insider attacks are the most elusive and perplexing issue that security professionals confront (p. 526). This complexity makes it difficult to predict and detect attacks.

The capability to predict attacks is important because if organizations have this ability, they can react to InT faster and more effectively. Schultz provided one of the earliest frameworks to identify and predict insider attacks. He provides a framework that defines "attack-related behaviors" and "symptoms," which he calls indicators (Schultz, 2002). These potential indicators are shown in Figure 2.

This framework proved to be useful in two ways. Firstly, each of these indicators became the subject of more pointed studies in the literature. Secondly, technical and behavioral observables have been produced by these succeeding studies. Yet, it should be noted that even though there are prediction and detection tools and techniques for insider attacks, there are not enough studies to conclude anything about the effectiveness of those tools and techniques.

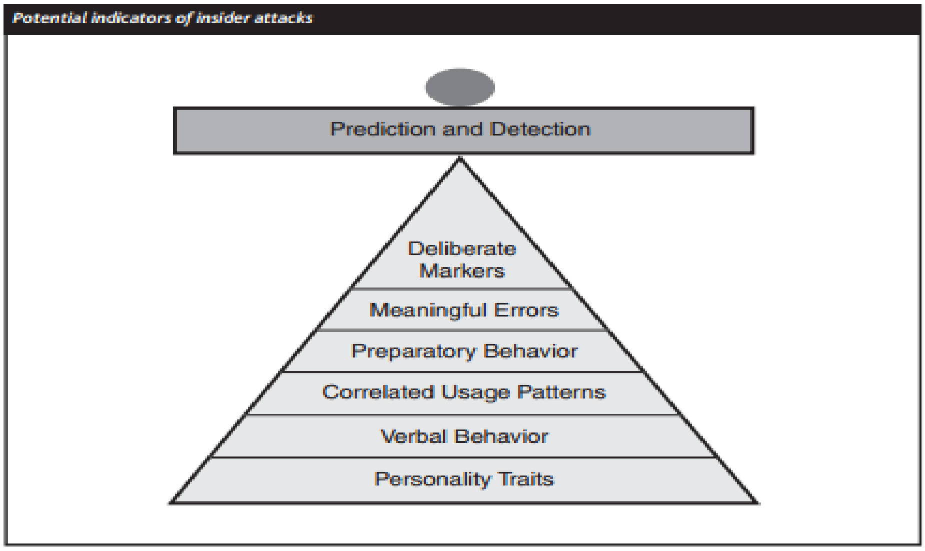


Figure 2. Potential Indicators of Insider Attacks. Source: Schultz (2002, p. 531).

F. INSIDER THREAT PREDICTION MODEL

Magklaras and Furnell provided one of the earliest models for predicting InT. This model "estimates the level of threat that is likely to originate from a particular insider by introducing a threat evaluation system based on certain profiles of user behavior" (Magklaras & Furnell, 2001, p. 62).

They start their study by proposing user misuse taxonomy, and then they provide an InT prediction tool (ITPT). The core component of threat prediction in the ITPT is the InT prediction model (ITPM). The model analyzes the users' footprints on the system for classifying them into the major insider categories, which are

> Possible intentional threat—The system has found evidence which suggests that it is very likely a particular user will initiate a specific misuse action.
>
> Potential accidental threat—The system has detected evidence that a user is about to perform a particular type of misuse, by accident.
>
> Suspicious—The system has detected a set of suspicious user activities, but it is not clear whether these actions indicate potential misuse activities.
>
> Harmless—There is no evidence that the user is likely to initiate any sort of undesirable action. (Magklaras & Furnell, 2001, p. 69)

The ITPM's value comes from qualifying and quantifying InT estimation metrics. The qualification means deciding which metrics to use and quantification means determining what relative weight those metrics will have. According to Caruso (2003), "They use a mathematical approach to determine values for each attribute and assign quantifiable values and adjustable metrics in order to predict the nature or level of a potential human threat" (p. 37).

$$\begin{aligned}
&\textbf{(top level)} && \mathrm{EPT}=\sum F_{\text{threat components}} \Rightarrow \\
& && \mathrm{EPT}= F_{\text{attrib}} + F_{\text{behavior}} + F_{\text{imsinfo}} \Rightarrow \\
&\textbf{(second level)} && \mathrm{EPT}= C_{\text{role}} + C_{\text{tools}} + C_{\text{hardware}} + F_{\text{behavior}} + F_{\text{imsinfo}} \Rightarrow \\
&\textbf{(third level)} && \mathrm{EPT}=C_{\text{role}} + C_{\text{data}} + C_{\text{hardware}} + F_{\text{knowledge}} + F_{\text{content}} + F_{\text{network}} + F_{\text{imsinfo}}
\end{aligned}$$

Figure 3. The Three-Layer ITPM Function Hierarchy.
Source: Magklaras and Furnell (2001, p. 72).

The details of the ITPT, ITPM, and Evaluated Potential Threat function are not the focus of this thesis. Although the model may seem complicated to utilize, the important contribution of Magklaras and Furnell’s study is that they provide a preliminary framework through which to analyze the insider problem.

G. PSYCHOSOCIAL INDICATORS FOR PREDICTION OF INSIDER THREATS

Although there exist numerous works to understand the psychology and the motivation of insiders, the difficulties of predicting insider attacks remains. In an effort to overcome such difficulties, Greitzer and Fricke (2010) propose a predictive framework that integrates cyber and psychosocial data. In this framework, prediction is enabled by a combination of demographic/organizational data and cyber-security audit data about system users. The authors warn that prediction is a very sensitive area and “any predictive analysis would have a number of gray areas” (Greitzer & Fricke, 2010, p. 87).

Based on interviews with human resources experts and other related managers who have knowledge about InT, Greitzer and Fricke (2010) provide twelve psychosocial indicators (the top five are presented in Table 1). They describe those indicators by “using examples or ‘proxies’ that are more readily observed than psychological constructs identified in the research literature (such as antisocial personality disorder or narcissism) that typically would not be available” (Greitzer & Fricke, 2010, p 101).

Table 1. Psychosocial Indicators (The Top Five of Twelve). Adapted from Greitzer and Fricke (2010, p. 102).

Indicator	Description
Disgruntlement	Employee observed to be dissatisfied in current position; chronic indications of discontent, such as strong negative feelings about being passed over for a promotion or being underpaid, undervalued; may have a poor fit with current job.
Accepting Feedback	The employee is observed to have a difficult time accepting criticism, tends to take criticism personally or becomes defensive when message is delivered. Employee has been observed being unwilling to acknowledge errors; or admitting to mistakes; may attempt to cover up errors through lying or deceit.
Anger Management Issues	The employee often allows anger to get pent up inside; employee has trouble managing lingering emotional feelings of anger or rage. Employee holds strong grudges.
Disengagement	The employee keeps to self, is detached, withdrawn and tends not to interact with individuals or groups; avoids meetings.
Disregard for Authority	The employee disregards rules, authority or policies. Employee feels above the rules or that they only apply to others.

At this point, it is important state that a psychosocial indicator becomes valuable only when the insider shows “extremely serious or grave manifestations of the indicator” (Bishop et al., 2010, p. 14).

III. SOCIO-TECHNICAL SYSTEMS THEORY, TRANSFER OF TECHNOLOGY, AND CULTURAL DIFFERENCES

A. SOCIO-TECHNICAL SYSTEM THEORY

Socio-technical system (STS) theory originates from works of Trist and Bamford (1951) at the Tavistock Institute of Human Relations in London. Their work focuses on interaction of social and technical systems within the United Kingdom coal mining industry that is presented with understanding of new coal mining machinery. At the end of their study, the message is that: “A technological change that appears quite rational from a purely engineering perspective can disrupt the existing social system so as to reduce greatly the anticipated benefits of the new technology” (Appelbaum, 2004, p. 458).

Trist and his colleagues’ work opened a new way to understand organizational functions. Baxter and Sommerville (2011) clearly state the overarching philosophy of STS theory in that for any organizational design, besides technical factors, human and social factors also must be taken into consideration. Better understanding “social factors affecting the ways that work is done and technical systems are used” contributes to organizational system design (Baxter & Sommerville, 2011, p. 4).

STS theory hypothesizes that organizations have two interdependent subsystems: the social and technical subsystems (Cartelli, 2007). The social subsystem is concerned with an “organization’s culture, norms, roles and communication patterns” (Appelbaum, 2004, p. 458). It includes value systems of the society where it resides and naturally reflects the national cultural dimension of its society. The technical subsystem deals with “the processes, tasks, and technology needed to transform inputs such as raw materials to outputs such as products” (Bostrom & Heinen, 1977, p. 14).

The core concept of the STS approach is that in order to maximize performance in any organizational system, the interdependency of technical and social subsystems must be explicitly recognized (Cartelli, 2007), a concept of “joint optimization” of subsystems. Joint optimization suggests that organizations must find a balance between the technology and the people utilizing this technology to design or redesign a process (Keating, 2001).

With its interdependent subsystems approach, STS theory provides a framework for technology related changes in organizations. In addition, because of its generality and adaptability to nearly all organizational situations, the STS approach provides a wide application area to organizations.

In most of the studies about socio-technical systems and organizational change, the word "change" is mostly used for system design or redesign in the organization. However, it is important to state that this approach is also very useful for "incorporating technological advancement into organizations" (Appelbaum, 2004, p. 452). Thus, STS theory, by accepting the interdependence of these two subsystems, helps organizations produce successful systems redesign, new system design, or transfer of technology.

B. TRANSFER OF TECHNOLOGY AND CULTURAL CONSTRAINTS ACROSS NATIONS

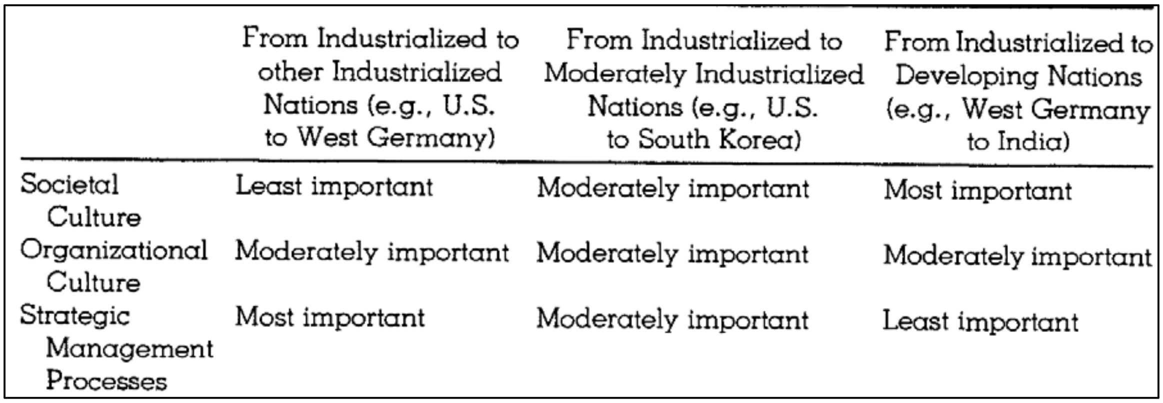
Since it differs from one discipline to another, providing a definition of transfer of technology (TOT) is challenging. Beginning from the 1950s, scholars and researchers have provided TOT definitions mostly based on the purpose of their research. In an attempt to provide a straightforward definition, Roessner (2000) identifies the TOT concept as "the movement of know-how, technical knowledge, or technology from one organizational setting to another" (p. 1). However, right after giving this plain definition Roessner admits that the term has been used widely for describing any organizational interactions that involve some form of technology exchange (Bozeman, 2000).

According to Bozeman (2000), most TOT related studies and publications have been provided by management scholars. Kedia and Bhagat (1988) explain that TOT has been considered in the area of international management. Following this explanation, they state that, through the end of the 1980s even though TOT literature highly emphasizes the effects of economic factors on TOT, surprisingly, there exists nearly no analyses of constraining effects of culture. Kedia and Bhagat emphasize the importance of cultural constraints on TOT as follows:

> Culture of the recipient organization, strategic management issues, and, perhaps more important, the cultural differences between the two nations involved, play significant roles in determining the efficacy of such transactions. (Kedia & Bhagat, 1988, p. 560)

For a better understanding of the effectiveness of TOT, they provide a conceptual framework that shows the relative importance of cultural differences across nations. According to this framework, the most important factor for effectiveness of transfer of technology between an industrialized nation and a developing nation is the societal culture. As one can see, while organizational culture is moderately important for such transactions, strategic management processes have least importance. The framework is depicted in Table 2.

Table 2. An Examination of the Relative Importance of Cultural Variation and Strategic Management Processes as Determinants of the Successful Transfer of Technology across Nations. Source: Kedia and Bhagat (1988, p. 560).



	From Industrialized to other Industrialized Nations (e.g., U.S. to West Germany)	From Industrialized to Moderately Industrialized Nations (e.g., U.S. to South Korea)	From Industrialized to Developing Nations (e.g., West Germany to India)
Societal Culture	Least important	Moderately important	Most important
Organizational Culture	Moderately important	Moderately important	Moderately important
Strategic Management Processes	Most important	Moderately important	Least important

More importantly for this thesis, in the same study, Kedia and Bhagat (1988) provided a model (Figure 4) for comprehending cultural constraints on TOT between countries.

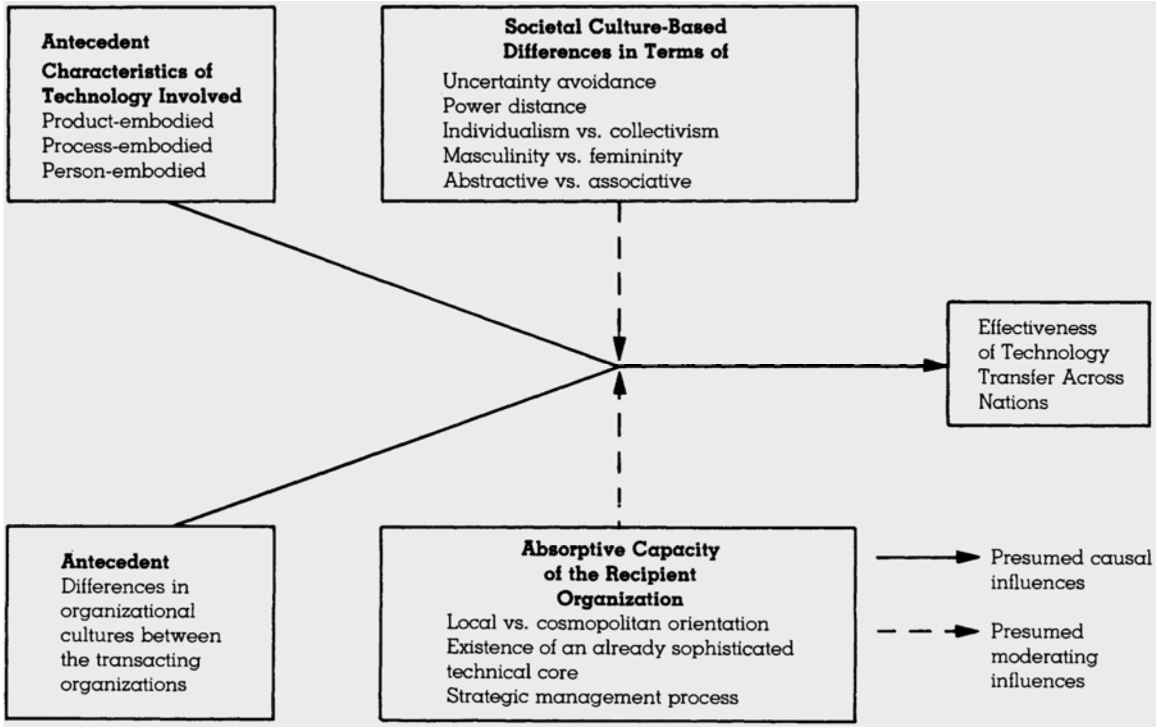

Antecedent Characteristics of Technology Involved
Product-embodied
Process-embodied
Person-embodied
Societal Culture-Based Differences in Terms of
Uncertainty avoidance
Power distance
Individualism vs. collectivism
Masculinity vs. femininity
Abstractive vs. associative
Effectiveness of Technology Transfer Across Nations
Antecedent
Differences in organizational cultures between the transacting organizations
Absorptive Capacity of the Recipient Organization
Local vs. cosmopolitan orientation
Existence of an already sophisticated technical core
Strategic management process
Presumed causal influences
Presumed moderating influences

Figure 4. A Conceptual Model for Understanding Cultural Constraints on Technology Transfers across Nations.
Source: Kedia and Bhagat (1988, p. 561).

This model shows two important antecedents that are "characteristics of technology involved" and "differences in organizational cultures between the transacting organizations." At this point, the importance of STS theory appears. The two antecedents of TOT correspond to two subsystems in STS theory: Characteristics of the involved technology antecedent corresponds to the technical subsystem, and the cultural differences between transacting organizations antecedent corresponds to the social subsystem. Even though Kedia and Bhagat do not explicitly state this fact, it can be clearly seen that their conceptual model points to the socio-technical system approach.

C. MODERATING FACTORS FOR TECHNOLOGY TRANSFER

Kedia and Bhagat's model defines two moderating factors for effectiveness of TOT. These factors are "societal culture-based differences" and "absorptive capacity of recipient organization." The first moderating factor points to five dimensions of national cultures that have a constraining effect on TOT. Four of these five dimensions originate from Hofstede's (1980) study. Only the "abstractive vs associative" dimension of culture comes from Glen and Glen's (1981) work. Since the focal point of this study is the analysis of the effects of Hofstede's national cultural dimensions on implementation of InT countermeasures, the details of Hofstede's framework and comparison of U.S. and Turkish cultures is provided in the following part of this chapter.

Although the absorptive capacity of a recipient organization is not the focus of this study, it would still be beneficial to provide a definition. Thus, absorptive capacity can be described as "the ability of a firm to recognize the value of new, external information, assimilate it, and apply it to commercial ends is critical to its innovative capabilities" (Cohen & Levinthal, 1990, p. 128). According to Zahra and George (2002), Kedia and Bhagat use the term absorptive capacity to indicate an organization's receptive capacity about technological changes. As can be inferred from the definition, the reason for excluding the effects of absorptive capacity is that it would shift the focus of this thesis from the effects of national cultural differences to organization specific factors such as orientation of the organization or level of sophisticated technology in the organization at that time.

D. HOFSTEDE'S MODEL: CULTURE AS THE SOFTWARE OF THE MIND

Since the purpose of this thesis is to adapt lessons learned from U.S. examples of InT countermeasures, it is necessary to use a model for cross-cultural considerations. This part of chapter discusses Geert Hofstede's "super classic" culture framework that transforms the amorphous idea of culture into a conformable structure.

In 1980 Geert Hofstede, a Dutch professor, published his best-selling book *Culture's Consequences*. Since then, the book has been cited more than 40,000 times in studies on culture and cross-cultural issues. Based on a broad survey (80,000 IBM employees from 72 countries) of work values, Hofstede provides a framework on culture. The reason why Hofstede's study has become so popular is that his framework "translated the rather amorphous idea of culture" into a conformable structure that was suitable to empirical research (Nakata, 2009, p. 3).

According to Hofstede (1980), culture is "the collective programming of the mind which distinguishes the members of one human group from another" and the heart of the culture is constituted by values that are "broad tendencies to prefer certain states of affairs over others" (pp. 13–26). Hofstede claims some cultural values that vary by levels exist in each country, and he provides five cultural dimensions related to those occurring values based on his findings.

Hofstede (1980) defines a dimension as "an aspect of a culture that can be measured relative to other cultures" and provides five dimensions of culture as "power distance," "individualism vs. collectivism," "masculinity vs. femininity," "uncertainty avoidance," and "Confucian dynamism" (p. 31). In 1991, Hofstede published another book, for a broader audience, and replaced the fifth dimension with the dimension of "long-term orientation" (Hofstede et al., 1991).

As mentioned before, Hofstede's model is based on a broad workplace survey (IBM) and this context is one of the main reasons for its inclusion in this study. Since this thesis focuses on insiders in organizations, Hofstede's model facilitates comparing U.S. and Turkish cultures in terms of organizational perspective. Specifically, power distance and uncertainty avoidance dimensions are utilized in order to discover potential problems and beneficial recommendations for adapting U.S. solution examples to TGCG.

The reason for selecting these two dimensions is that "power distance and uncertainty avoidance in particular affect our thinking about organizations" (Hofstede, Hofstede & Minkov, 2010, p. 302).

> Organizing always requires answering two questions: (1) who has the power to decide what? and (2) what rules or procedures will be followed to attain the desired ends? The answer to first question is influenced by cultural norms of power distance; the answer to second question, by cultural and norms about uncertainty avoidance. (Hofstede et al., 2010, p. 302)

Individualism and masculinity dimensions are mostly related to people, and in our case those dimensions are mostly related to an insider's profile (psychologically and psychosocially) in the workplace. Even though individualism and masculinity dimensions are used in this thesis when necessary, this topic could be further explored in future work. The following sections include detailed explanations of “power distance” and “uncertainty avoidance,” and brief definitions of “masculinity vs. femininity” and “individualism vs. collectivism.”

1. Power Distance

“Power distance” is concerned with inequalities within society. Some members of society have more power than others in terms of physical and intellectual capabilities, wealth, and status. Inequality in distribution of power is the source of power distance. Hofstede and his colleagues explain power distances based on “the value system of the less powerful members” (Hofstede et al., 2010, p. 61).

> The power distance can be defined as the extent to which the less powerful members of institutions and organizations within a country expect and accept that power is distributed unequally. Institutions are the basic elements of the society such as the family, the school, and the community; organizations are the places where people work. (Hofstede et al., 2010, p. 61)

The power distance index (PDI) is used to explain this dimension and dependence relationship in a country and determines the PDI score (Hofstede et al., 2010). To illustrate this relationship, in small-power-distance countries (low PDI), subordinates’ dependency on superiors is limited and “the emotional distance” between them is rather small, which means subordinates feel comfortable enough to contradict their bosses. In large-power-distance countries (high PDI), dependence is high and emotional distance is large between bosses and subordinates. Large emotional distance decreases the likelihood of approaching and contradicting bosses (Hofstede et al., 2010).

In the PDI scale Turkey’s score (66) is higher than the United States’ score (40). On this scale Malaysia and Slovakia have the highest (104) scores and Austria has the lowest score (11). It is important to realize that because of the method used by researchers, the PDI scores represent relative positions of the countries rather than their absolute positions (Hofstede et al., 2010). This means Turkey is a large-power-distance country relative to the United States, which is a small-power-distance country. Table 3 provides important differences between small and large power distance cultures on work related issues.

Table 3. Key Differences between Small and Large Power Distance Societies in the Workplace. Source: Hofstede et al. (2010, p. 76).

Small Power Distance	**Large Power Distance**
Hierarchy in organizations means an inequality of roles, established for convenience	Hierarchy in organizations reflects existential inequality between higher and lower levels
Decentralization is popular	Centralization is popular
There are fewer supervisory personnel	There are more supervisory personnel
There is a narrow salary range between the top and the bottom of the organization	There is a wide salary range between the top and the bottom of the organization
Managers rely on their own experience and on subordinates	Managers rely on superiors and on formal rules
Subordinates expect to be consulted	Subordinates expect to be told what to do
The ideal boss is a resourceful democrat	The ideal boss is a benevolent autocrat, or good father.
Subordinate-superior relations are pragmatic	Subordinate-superior relations are emotional
Privileges and status symbols are frowned upon	Privileges and status symbols are normal and popular
Manual work has the same status as office work	White-collar jobs are valued more than blue-collar jobs

2. Uncertainty Avoidance

Uncertainty avoidance is concerned with how people handle ambiguity in their organizations. Unclear, unstructured, and unpredictable situations create a sense of uneasiness or anxiety. The way people try to avoid such situations is by adopting strict rules. However, the extent of adoption varies by culture. A useful definition of this dimension is as follows:

> the extent to which the members of a culture feel threatened by ambiguous or unknown situations. This feeling is, among other manifestations, expressed through nervous stress and in a need for predictability: a need for written and unwritten rules. (Hofstede et al., 2010, p. 191)

The countries that score high on the uncertainty avoidance index (UAI) take a strong position against uncertainty. They emotionally need rules, and they have a strong belief in experts and technical solutions. Subordinates expect clear instructions from their superiors to perform their jobs. They usually do not fear taking familiar risks but avoid taking unfamiliar risks (Hofstede et al., 2010).

A low uncertainty score on the UAI scale means weak uncertainty avoidance. In weak uncertainty avoidant countries, people think the regulations should exist only if they are needed and despise excessive rules. They are more tolerant of ambiguity and chaos, and they feel more comfortable taking unfamiliar risks (Hofstede et al., 2010).

On the UAI scale Turkey's score (85) is higher than the U.S. score (46). This means Turkey is a strong uncertainty avoidant country and the United States is a weak uncertainty avoidant country. Table 4 provides key differences in the workplace related issues.

Table 4. Key Differences between Weak and Strong Uncertainty Avoidance Societies in the Work, Organization, and Motivation. Source: Hofstede et al. (2010, p. 217).

Weak Uncertainty Avoidance	**Strong Uncertainty Avoidance**
More changes of employer, shorter service There should be no more rules than strictly necessary Work hard only when needed Time is a framework for orientation Tolerance for ambiguity and chaos Belief in generalists and common sense Top managers are concerned with strategy More new trademarks Focus on decision process Entrepreneurs are relatively free from rules There are fewer self-employed people Better at invention, worse at implementation Motivation by achievement and esteem or belonging	Fewer changes of employer, longer service, more difficult work-life balance There is an emotional need for rules, even if they will not work There is an emotional need to be busy and an inner urge to work hard Time is money Need for precision and formalization Belief in experts and technical solutions Top managers are concerned with daily operations Fewer new trademarks Focus on decision content Entrepreneurs are constrained by existing rules There are more self-employed people Worse at invention, better at implementation Motivation by security and esteem or belonging

3. Individualism versus Collectivism

This dimension concerns the social links between a person and others in a community. This relationship appears to be loose in individualist societies, whereas in collectivist societies it appears to be tight. Individual achievement and freedom is more important to those in individualist societies. People in collectivist societies attach more importance to the greater good of the society. The definition of these terms is as follows:

> Individualism pertains to societies in which the ties between individuals are loose: everyone is expected to look after himself or herself and his or her immediate family. Collectivism as its opposite pertains to societies in which people from birth onwards are integrated into strong, cohesive in groups, which throughout people's lifetime continue to protect them in exchange for unquestioning loyalty. (Hofstede et al., 2010, p. 92)

Hofstede and his colleagues provide an individualism index (INV) to show relative positions of countries in terms of individualism. The countries that score high on this scale are accepted as individualist societies and low scoring countries are accepted as collectivist societies. Some major implications for the individualism vs. collectivism dimension from the 2010 study by Hofstede et al. are that in individualist societies, employees are expected to follow their own self-interest in the workplace. As a normal workplace environment in these societies, the employer's and employees' interests should meet at an acceptable point. However, in collectivist countries, employees tend to act for the benefit of group that they belong to. In case of collision of group interest and self-interest, employees are expected select group interest.

Interestingly, the workplace relationship in collectivist countries resembles family relationships. Employees have protection in exchange for their loyalty to this family, and usually poor performance does not require job termination. In contrast, termination of job because of poor performance or better pay from another company is the normal response in individualist countries.

In a comparison of Turkey and the United States, Turkey scores much lower (37) than the United States (91) on the INV index, which means Turkey is a "collectivist society" and the United States is an "individualist society." In fact, the United States has the highest score in this index. Table 5 provides key differences in the work, education, and technology related issues in terms of the INV index.

Table 5. Key Differences between Collectivist and Individualist Societies - Workplace, School, and Information and Communication Technologies. Source: Hofstede et al. (2010, p. 124).

Collectivist	**Individualist**
Students speak up in class only when sanctioned by the group	Students are expected to individually speak up in class
The purpose of education is learning how to do	The purpose of education is learning how to learn
Diplomas provide entry to higher status groups	Diplomas increase economic worth and/or self-respect
Occupational mobility is lower	Occupational mobility is higher
Employees are members of in-groups who will pursue the in-group's interest	Employees are "economic persons" who will pursue the employer's interest if it coincides with their self-interest
Hiring and promotion decisions take employee's in-group into account	Hiring and promotion decisions are supposed to be based on skills and rules only
The employer-employee relationship is basically moral, like a family link	The employer-employee relationship is a contract between parties in a labor market
Management is management of groups	Management is management of individuals
Direct appraisal of subordinates spoils harmony	Management training teaches the honest sharing of feelings
In-group customers get better treatment (particularism)	Every customer should get the same treatment (universalism)
Relationship prevails over task	Task prevails over relationship
The Internet and email are less attractive and less frequently used	The Internet and email hold strong appeal and are frequently used to link individuals

4. Masculinity versus Femininity

The relationship between gender and workplace issues is the focus of another cultural dimension. However, this relationship is not about being male or female. Instead, it is about the value system of societies. Masculinity of a society is about its predominant masculine values, such as assertiveness and competitiveness in daily life and in the workplace. This dimension is defined as follows in Hofstede and his colleagues' study.

> A society is called masculine when emotional gender roles are clearly distinct: men are supposed to be assertive, tough, and focused on material success, whereas women are supposed to be more modest, tender, and concerned with the quality of life. A society is called feminine when emotional gender roles overlap: both men and women are supposed to be modest, tender, and concerned with the quality of life. (Hofstede et al., 2010, p. 140)

Similar to the individualism index, the masculinity index (MAS) that is presented by Hofstede et al. (2010) shows relative positions of countries with regard to masculinity. High scores on the masculinity index point to masculine societies and low scores point to relatively feminine societies. Some important differences for workplace issues that are discussed in Hofstede et al. (2010) study are briefly mentioned here.

Firstly, even the definition of management changes based on this dimension. For example, for feminine societies management requires intuition and consensus whereas in masculine societies it requires decisiveness and aggressiveness. Secondly, workplace conflicts are handled differently according to characteristics of society. In masculine societies people let the strongest win. In feminine societies conflicts are handled with compromise and negotiation. Finally, rewarding employees based on achievement differs considerably. In masculine societies, rewards are delivered to employees based on equity that is "to everyone according to performance." Contrary to equity, organizations reward employees based on equality, that is, "to everyone according to need" (Hofstede et al., 2010, p. 167).

Even though the scores are close to each other, the United States (MAS score: 62) is a masculine society when compared to Turkey (MAS score: 45). To give a sense of the relative difference, Slovakia has the highest score in MAS at 110 and Sweden has the lowest score at only 5. Table 6 shows primary dissimilarities between masculine and feminine cultures in work related issues.

Table 6. Key Differences between Feminine and Masculine Societies in the Workplace. Source: Hofstede et al. (2010, p. 170).

Feminine	**Masculine**
Management as ménage: intuition and consensus	Management as manège: decisive and aggressive
Resolution of conflicts by compromise and negotiation	Resolution of conflicts by letting the strongest win
Rewards are based on equality	Rewards are based on equity
Preference for smaller organizations	Preference for larger organizations
People work in order to live	People live in order to work
More leisure time is preferred over more money	More money is preferred over more leisure time
Careers are optional for both genders	Careers are compulsory for men, optional for women
There is a higher share of working women in professional jobs	There is a lower share of working women in professional jobs
Humanization of work by contact and cooperation	Humanization of work by job content enrichment
Competitive agriculture and service industries	Competitive manufacturing and bulk chemistry

E. CONCLUSION

According to Kedia and Bhagat's (1988) approach, implementation of a new technical capability (in our case it is InT risk mitigation capability) to another organization in a different country can be accepted as TOT. In addition, as explained before, these two researchers implicitly utilize the socio-technical system approach for their conceptual model.

By combining socio-technical systems theory and the technology transfer approach, we claim that technical measures for countering InT are related characteristics of the technology antecedent (technical subsystem), and non-technical measures are related to the cultural differences of transacting organizations antecedent (social subsystem) of Kedia and Bhagat's model. After accepting this relationship, we use the moderating factor of societal culture-based differences to analyze cultural constraints on implementing InT countermeasures to TGCG.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. NON-TECHNICAL CONTROLS AGAINST INSIDER THREATS AND EFFECTS OF TURKISH CULTURE

A. UNITED STATES EFFORTS AGAINST INSIDER THREATS

Industries' and government organizations' research on InT and mitigation strategies against malicious insiders has been going on progressively since the beginning of the 2000s. However, in the past six years, multiple events, such as the Fort Hood Shootings (2009) and the WikiLeaks phenomenon (2011) have directed the attention of the United States government from the highest level.

In October 2011, the Obama administration released Executive Order 13587, directing "structural reforms to improve the security of classified networks and the responsible sharing and safeguarding of classified information" (Executive Order No. 13587, 2011, p. 1). In this executive order, President Obama directs the establishment of a national Insider Threat Task Force (ITTF) and orders federal agencies to build an InT program compatible with the standards developed by this task force. According to the executive order, the responsibility of ITTF is to build a Government-wide InT program to counter InT that includes protection of classified information from "exploitation, compromise, or other unauthorized disclosure" (Executive Order No. 13587, 2011, p. 3).

After one year of effort on security reviews and coordination between agencies, the National ITTF (NITTF) developed the "National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs," and it was released as a Presidential Memorandum (Obama, 2012) in November 2012. This memo explains the aims of national InT policy, delegates responsibilities to federal agencies and departments, restates the purpose and responsibilities of ITTF, and provides minimum standards for InT programs of governmental organizations. Some of the minimum standards include:

- Designation of Senior Officials for insider threat programs and responsibilities of these officials
- Building and maintaining an insider threat analysis and responding capability
- Assigning trained personnel to the insider threat programs
- Establishing procedures for sharing information between related organizations for insider threat purposes
- Monitoring user activities on networks
- Training all cleared employees for insider threat awareness (Obama, 2012, pp. 1–4)

In fact, some serious events proved the necessity of White House-level attention to the InT. As an example of unauthorized disclosure of classified information by malicious insider, Edward J. Snowden, a computer professional and former U.S. Central Intelligence Agency and government worker, also leaked information from the U.S. National Security Agency and United Kingdom government in 2013 (Dedman, Brunker, & Cole, 2014).

Like the Fort Hood Shootings in 2009, another InT event involving violent behavior, the Washington Navy Yard Shootings (2012), lead to the establishment of the DOD Insider Threat Management and Analysis Center (DITMAC). One of the key recommendations of Washington Navy Yard Shootings reviews was the establishment of DITMAC with responsibility “to assess, recommend intervention or mitigation, and oversee case action on threats that insiders may pose to their colleagues and/or DOD missions and resources” (Hagel, 2014, p. 1).

Parallel to these developments, DOD released a directive to establish policy, assign responsibilities to its components, and start an InT program to meet the minimum standards in order to counter insiders (DOD, 2014). The main purpose of the DOD InT program is clearly stated in the directive as follows:

> Through an integrated capability to monitor and audit information for insider threat detection and mitigation, the DOD Insider Threat Program will gather, integrate, review, assess, and respond to information derived from CI [counterintelligence], security, cybersecurity, civilian and military

> personnel management, workplace violence, AT [antiterrorism]risk management, LE [law enforcement], the monitoring of user activity on DOD information networks, and other sources as necessary and appropriate to identify, mitigate, and counter insider threats. (DOD, 2014, p. 2)

The previously mentioned executive orders, memorandums, and directives are very high-level documents that provide first and rapid steps against InT. There exist dozens of similar guiding documents partially or totally dedicated to mitigate the risk posed by insiders. The focus of this chapter is the conceptual implementation of common mitigation strategies and best practices against malicious insiders considering cultural differences of TGCG. Those mitigation strategies and best practices are derived from scholarly works and technical reports (e.g., CERT publications), guiding documents (e.g., Presidential Memorandum on InT), and industry recommendations (e.g., SIFMA InT Best Practices Guide). The mapping of best practices is presented in Appendix A.

B. PRACTICE #1 – CONDUCT ENTERPRISE-WIDE RISK ASSESSMENT

Most organizations focus on protecting their information against unauthorized external access and usually do not pay much attention to the InT with the notion of “this can’t happen to me.” Instead, organizations should carefully determine potential insider attacks and the impact of those attacks to any of their assets.

It is neither an easy nor a cheap task to protect organizations’ information, information systems, or assets from external or internal attacks. For many organizations, especially large ones, fully protecting the entire organization’s assets against all threats is not practical and, in fact, it is not achievable. A reasonable approach to the insider problem for organization should include increasing security efforts relative to criticality of the information or the asset to be protected. Extra controls should be applied to the most critical assets.

Keeping this challenge in mind, it is very crucial to conduct an enterprise-wide risk assessment with respect to InT. This assessment would enable the organization to address the critical information (national secrets, confidential or proprietary information, financial data, personally identifiable information, or mission-critical data) and assets, threats to these assets and information, and possible impacts of the insider attacks if they happen. Addressing the critical information and assets is not enough for an effective risk assessment. An effective enterprise-wide risk assessment must include vulnerabilities of addressed critical information and assets.

It is also important to define organization boundaries broadly enough. These boundaries should include employees and other workers such as contractors, consultants, and outsource service providers who have rights to access computer systems and data assets of the organization.

For an effective enterprise-wide risk assessment, organizations are required to identify what to protect, in other words find their "crown jewels," and understand where this sensitive information lives. This would make it easier to watch concerning insider behavior and associated risk once the critical assets are identified, classified, and located in the organization network. Risk assessment should also include not only who has access to the "crown jewels" but also who should have access.

Effects of Turkish Culture on Implementation

Large-power-distance scoring societies, such as Turkey, are prone to have a more collectivist nature than small PDI scoring societies (Hofstede et al., 2010). Hofstede and his colleagues clearly show that Turkey is more collectivist than the United States. In collectivist societies, employees see themselves as members of the in-group and seek the interest of their in-group even when this interest collides with employees' interest. This in-group relationship resembles a family relationship between employees and employer with "mutual obligation of protection in exchange for loyalty" (Hofstede et al., 2010, p. 120).

This mindset can cause missing important pieces in enterprise-wide risk assessment because loyalty between these counterparts in the workplace is an important characteristic of collectivist societies. The employees who make the risk assessment may not make sense of why and how insiders harm the organization and may overlook InT because assessors would see insiders as a member of their family. In addition, assessors may hesitate to articulate the threats posed by employees, which inevitably decreases the effectiveness of the risk assessment.

The high uncertainty avoidance characteristic of Turkey also may affect risk assessment of InT in many ways, but one should not confuse uncertainty avoidance with risk avoidance. A reasonably high risk-avoidance characteristic could be useful for more realistic risk assessment of InT. High uncertainty avoidance could lead to better determination of plans and procedures for mitigating InT after this proper risk assessment.

In high uncertainty avoidance societies employees are less willing to change their jobs and are apt to seek longer service times (Hofstede et al., 2010). Until the end of their service in the organization, they work in different departments and at varying levels that gives them deep knowledge about the organization and various access rights to different parts of the information systems. When conducting a risk assessment, organizations in high uncertainty avoidance countries should consider the possibility of conveying information to new positions and negligence in updating access rights

Lastly, in high uncertainty avoidance societies, people are prone to have confidence in experts and technological solutions (Hofstede et al., 2010). This feeling of confidence is likely to create a false sense of having sufficient controls against InT in the risk assessment phase. This could seriously hamper the assessment because the trusted expert or the administrator of the technological solution could be the source of the threat.

C. PRACTICE #2 – DEFINE POLICIES AND PROCEDURES, ENFORCE CONSISTENTLY

Most of the mitigation strategies and best practices documents reviewed for this study require maintaining sound policies and procedures against InT and enforcing these policies consistently. According to CERT researchers, policies should clearly address the following issues specifically:

- Acceptable use of the organization’s systems, information, and resources
- Use of privileged or administrator accounts

- Ownership of information created as a work product
- Evaluation of employee performance, including requirements for promotion and financial reward
- Bonuses
- Processes and procedures for addressing employee grievances (Silowash et al., 2012, p. 13)

Policy document should be brief, plain, and understandable and should include the reasoning behind the policy if possible. A concise and coherent policy not only forces malicious insiders to think twice before committing an insider crime, but also can remove or at least decrease the misunderstandings and unwitting harm that can be caused by reckless or ignorant employees.

To get the desired results from policies and procedures, organizations must ensure those policies and their implementations/enforcements are included in InT awareness and periodic trainings. Besides, organizations should keep evidence that proves employees and contractors have read and agreed on policies. Organizations usually get this evidence in the hiring processes. However, organizations are living systems, and they should review and update policies and procedures periodically. Changes in the policies or procedures should be reflected on evidence documents such as nondisclosure agreements for new and existing employees.

Consistent enforcement of the InT policies is very important in terms of fostering a sense of justice in workplace. Policies should be applied to all stakeholders including managers and system administrators. Otherwise, a feeling of injustice can breed resentment and increase the likelihood of potential insider attacks.

Special attention should be given to the users who have broad access rights to the information systems. Those individuals (e.g., system administrators, power users) present a special challenge to the organization, and special policies should be considered for them. These separate and special policies should address a different normal behavior baseline other than normal users have.

Effects of Turkish Culture on Implementation

In large PDI scoring countries, subordinates look for specific orders to perform their tasks in the workplace. This expectation would limit the contribution of subordinates to the process of creating policies and procedures because they believe the superiors have the power, which is knowledge about InT in this case, and these power-holders should state the policies and procedures explicitly.

According to Hofstede et al. (2010), in large PDI scoring societies there are more supervisors and managers relying on formal rules. This can have two kinds of effect. Firstly, the buy-in decision of supervisors becomes more important when creating policies and procedures. Secondly, superiors and managers feel existentially unequal to their employees, and inevitably management demands privileged access rights to the information systems.

As mentioned before, a special policy should be considered for system administrators and privileged users. Superiors and managers who have those privileges may resent special policies against them and can be inclined to circumvent the policies and procedures. Organizations should identify and have closer monitoring of individuals who are in this position.

Employees need rules and feel more comfortable in workplaces that are more structured environments in strong uncertainty avoidant societies. In addition, they look for precision and formalization. To fulfill those needs, the number of policies and procedures can be more than necessary and they can be over detailed. This situation may harm the policies and procedures' ability to be concise and coherent. As another effect, reliance on the technical solutions in strong uncertainty avoidant countries can lead missing some important points that should be stated clearly in the policies or procedures.

The need for rules and the communication of these rules to the employees are two different factors to consider. Employees may need rules emotionally even if these rules will not work, but communication of the rules matters. According to Hofstede and his colleagues (2010), in collectivist countries like Turkey, high-context communication prevails. Referring to Edward T. Hall, Flynn, Huth, Trzeciak, and Buttles (2013) state that “high-context cultures communicate in implicit ways, relying on presumed context of cultural information to fill the gaps” (p. 3). In order to decrease misunderstandings and unwitting harm, organizations should not rely on cultural information to complete the missing pieces of context. Instead, they should clearly and explicitly communicate policies and procedures.

D. PRACTICE #3 – DEVELOP A FORMALIZED INSIDER THREAT PROGRAM

The first thing to do that was directed in Executive Order 13587 and the Presidential Memorandum to the all U.S. agencies is the establishment of an InT program and assignment of a senior officer to provide management and oversight of the program. Countering InT seems to be the responsibility of security and IT departments. The senior official’s responsibility should be establishing the InT program that will link other areas of the organization.

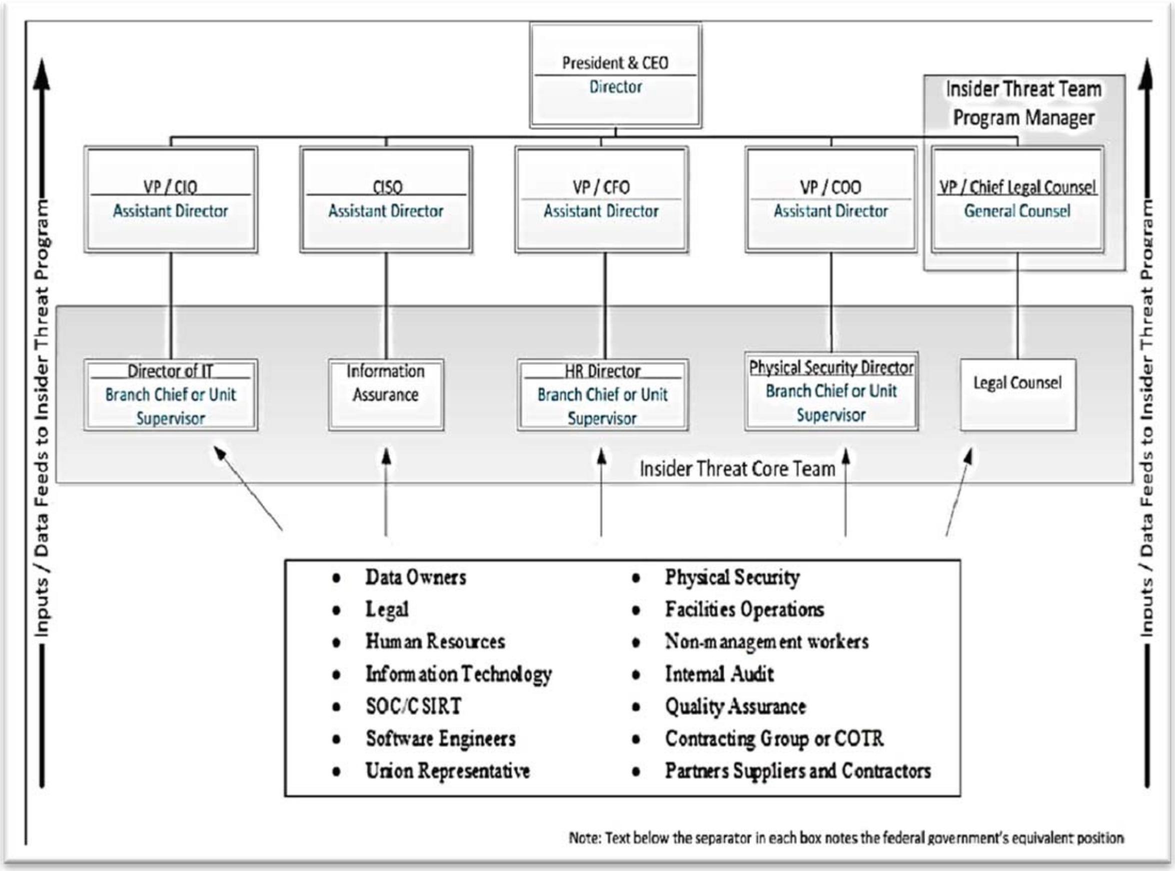
To mitigate InT risks, an InT program should broadly cover organizations’ boundaries and should define roles and responsibilities openly. In this regard, the goal of an InT program should be providing

- Criteria for defining insiders
- A consistent procedure for implementing technical and nontechnical controls to prevent malicious insider behavior
- A response plan in the event an insider does harm the organization (Flynn et al., 2013, p. 9)

Legal counseling is very important for the establishment of the program because the organization should be sure not to violate any personal rights of its employees during the gathering of information and maintaining evidence.

A team approach is very important for an InT program. The program should be executed by an InT team. Every organization can have different departments that deal with insider risk at varying levels, and it is critical to identify and include stakeholders in this team. A formal InT team can include members of the other teams in the organization and does not need to be a dedicated entity. However, its location must be determined, and its members and their roles and responsibilities must be defined before an insider incident occurs.

The CERT researchers provide a structure (Figure 5) that includes a core InT team, which has mostly the same members that are recommended by other works, and other stakeholders within an organization who can present their information and perspectives about potential InT as a part of mitigating the risk of insider attacks. In Figure 5, the teams that are presented under the core InT team do not have to be involved in every insider incident. Instead, an organization should consider in which phases (deterring, prevention, detection, and responding) these teams must be involved in the efforts.



Note: Text below the separator in each box notes the federal government's equivalent position

Figure 5. Inputs and Data Feeds to Insider Threat Program.
Source: Silowash et al. (2012, p. 75).

Effects of Turkish Culture on Implementation

According to Hofstede et al. (2010), no empirical or theoretical studies exist claiming that power distance has effects on the efficiency of organizations. However, large-power-distance countries like Turkey can be better at tasks requiring discipline. For this reason, building an InT team, including required members and participation at the regular meetings can be easier. However, participation does not necessarily mean there is contribution. Subordinates' contribution to the team and InT program may be limited because of the nature of the large-power-distance societies.

As mentioned previously, an important goal of an InT program is to provide criteria for defining insiders. In collectivist societies, a workplace is seen emotionally as an in-group itself. This trust-based mindset coming from family and school has potential to affect negatively the process of defining insiders. Organizations should consider including counseling firms in the development of the InT program in order to have an external perspective on the in-group members.

The core InT team members who will carry out the InT program should be selected carefully. Those members can be members of other teams, but they should not have conflicts between each other. The consideration behind this is that, as Hofstede et al. (2010) state, in collectivist societies "the personal relationship prevails over task and should be established first." If this consideration is overlooked, employees could focus on conflicts instead of the task itself, which can harm the program.

The legal considerations are not a part of this study. However, it is a fact that organizations in high UAI scoring countries are likely to have more formal laws and regulations, even if they are dysfunctional or ineffective, that address duties and rights of the employees in workplaces. Therefore, legal counsel must be delicate when helping to build a legitimate InT program that protects the civil liberties of the employees.

E. PRACTICE #4 – PROVIDE INSIDER THREAT AWARENESS TRAINING

Once an InT program is initiated and policies and procedures are defined, these policies and procedures are required to be communicated to the employees, and this information should be included in security awareness trainings. All the controls against InT will be ineffective and short-lived without the complete understanding of employees. All employees should understand that insider crimes could have very serious consequences for their organization, such as loss of reputation, decrease in stock value, or even danger to future existence.

The percentage of potential malicious insiders could be very low, but the remaining majority of personnel must be made aware and properly trained. In this regard, InT program managers should definitely include InT components into security awareness training and be sure that all employees receive formal training at least once a year. New employees and contractors should be trained in insider issues before they have access to an organization's computer systems.

InT awareness training should inform employees about criminal social networking, social engineering, and recruitment by other insiders or outsiders. The training provided about these incidents and their potential consequences could alert employees and increase the probability of reporting to the management. With regard to reporting, organizations should include how to report an insider issue confidentially, without fear of repercussion.

The InT training should communicate acceptable-use of computer systems and notify employees that they are being monitored on the system. Employees should understand that they "do not have any expectation of privacy on work computers and devices" (SIFMA, 2014, p. 14). In addition, this fact should be clearly stated in the use of information systems policy. An additional training session can be planned for system administrators and privileged users because they should be notified that they will get closer monitoring.

Awareness trainings should make employees understand they have to protect the organization's information and that compromise of this information will have legal consequences. In addition, employees must understand that any piece of information, program, or asset they produce or they are responsible for belongs to the organization. Misunderstanding of this rule can lead to unintentional insider incidents.

For a successful InT program, employees are required to identify and report insiders. Nevertheless, there is no single profile for insiders. To identify malicious insiders, InT trainings should focus on attributes of behaviors rather than their stereotypical characteristics. According to Silowash and his colleagues those behaviors include:

- Threatening the organization or bragging about the damage the insider could do to the organization
- Downloading large amounts of data within 30 days of resignation
- Using the organization's resources for a side business or discussing starting a competing business with co-workers
- Attempting to gain employees' passwords or to obtain access through trickery or exploitation of a trusted relationship (often called "social engineering") (Silowash et al., 2012, p. 17)

Finally, security awareness trainings should be continuous. Formal training once or twice a year is necessary but not sufficient. Employees should be informed continuously with posters, banners, and alert emails throughout the year.

Effects of Turkish Culture on Implementation

In Turkey, as a high-power-distance country, training is instructor centered. Instructors are respected and even feared. The information that an instructor provides is seen as the only path to follow in order to have success. With this in mind, the quality of the trainings depends on the excellence and knowledge of the instructor. The instructors who will present the formal part of the InT awareness training should have substantial information on the InT subjects because the audience would expect great knowledge from them. Brief explanations and short presentations of related documents would not be enough to increase awareness of InT.

The attendance of managers and superiors at the InT trainings or their support for other training materials, such as posters, is important for increasing organizational buy-in. This is a normal procedure in small-power-distance societies because employees think of themselves as existentially equal with their superiors. Superiors' attendance at the trainings is normal to them. In high PDI scoring societies like Turkey, subordinates will have a stronger feeling for the importance of the InT training if they see their bosses in the same training.

The goal of the education or training differs in collectivist and individualist cultures. In collectivist societies the goal is to know how to do something while it is to know how to learn something in individualist countries (Hofstede et al., 2010). In this regard, continuous learning becomes more important for Turkey, which has a collectivist culture according to Hofstede's study. It is likely that employees would wait until the next formal training to get more information about InT instead of learning something on the subject themselves. Therefore, continuous learning will keep employees' InT awareness at the desired level.

One of the important pieces of InT mitigation is the detection of behavioral indicators of an insider and reporting them confidentially. Organizations should define how to confidentially report indicative behaviors precisely in their InT program because high uncertainty avoidance societies naturally would need more rules to overcome ambiguity in sensitive areas like whistle blowing. The steps for reporting indications of potential InT behaviors must be taught to employees explicitly and in detail. If employees feel ambiguity or uncertainty in the reporting process, they could refrain from reporting due to fear of being revealed.

F. PRACTICE #5 – REVIEW EMPLOYEE TERMINATION PROCESSES

CERT researchers, based on their insider incident database, state that many insider IT sabotage incidents happen because of organizations' insufficient or bad practices around employee termination procedures, especially before and after 30 days from departure of employees (Cappelli et al., 2012). To mitigate these kinds of risks, organizations should have standard termination procedures, should communicate these to the entire organization, and must strictly implement them in every case. High-risk profiled employees must be given closer attention upon their termination.

Organizations should use a termination checklist that includes related areas (e.g., physical security, IT security, information assurance, finance, configuration management, human resources, etc.). This checklist will be useful, making it mandatory for an employee to follow before his departure (Silowash et al., 2012). A termination procedure should include, but not be limited to, the following aspects:

- All physical properties of the organization must be collected (access cards, badges, keys, authentication tokens, mobile devices, laptops).
- All accounts of the employee must be closed.
- All agreements about intellectual property and nondisclosure must be reaffirmed. In fact, this is an opportunity to remind the employee of his or her responsibilities even after leaving the company.
- All passwords of shared accounts, network devices, and test accounts must be changed. If the departing employee is a system administrator or privileged user, all privileged user account passwords should be reset to prevent against use of potential compromised accounts.
- All connections that enable an employee to access the organization's information systems remotely, such as VPN, must be disabled.
- In addition to previous controls, an employee's all access logs, email activities, network activities, and unusual traffic flow must be monitored closely 30 days before and after termination.
- Finally, all employees must be notified when an employee has departed. (Silowash et al., 2012, pp. 65–68)

Even though this can be seen as a privacy issue, the notification does not need to include how and why the employee is terminated. The name of the terminated employee and a warning about not disclosing any confidential information would be sufficient for the notification. This small but efficient notification can prevent unintentional disclosure of classified information, limits social engineering, and hinders a terminated person's entrance to the organization's facilities and systems.

These technical and administrative controls ensure that departing employees can no longer access organization assets, which helps mitigate the risk of insider attacks upon termination.

Effects of Turkish Culture on Implementation

Considering Hofstede and his colleagues' (2010) cultural dimensions, it can be said that individualist-collectivist and uncertainty avoidance characteristics dimensions affect employee termination procedures more than other dimensions. These two dimensions put more emphasis on social consequences of termination rather than legal consequences.

In collectivist countries like Turkey, violation of rules or social norms (excluding legal consequences) in the workplace raises the feeling of shame for the employee. In an individualist society, the same situation leads to the feeling of guilt. According to Hofstede et al. (2010) “shame is social in nature, whereas guilt is individual” (p. 110). If the violations of the rules are known to others, this leads to shame in collectivist societies. The important point here is that an organization’s termination procedures and behaviors related to departing employees should not create too much shame and embarrassment, which can lead to feelings of revenge against the organization. This kind of bad experience can increase the likelihood of committing insider crimes that can the harm the organization. In this respect, organizations should focus on the fault and avoid exposing a departing employee in front of the rest of the organization.

As stated in the effects of the Turkish culture on the adoption of Practice One, in high uncertainty avoidance countries such as Turkey employees tends to stay in their jobs for longer service times. A combination of this characteristic with the collectivist nature of Turkey inevitably leads to very close family-like relationships between employees in different departments of the organization. A malicious insider can use these close relationships after his termination to get information and access the organization’s information systems or physical facilities. In other words, organizations become more vulnerable to unintentional disclosure of classified information through social networking and social engineering. For this reason, organizations should inform their employees to be more vigilant against these kinds of incidents.

THIS PAGE INTENTIONALLY LEFT BLANK

V. TECHNICAL CONTROLS, INSIDER HUB ORGANIZATION, AND EFFECTS OF TURKISH CULTURE

A. PRACTICE #6 – MONITORING USER ACTIVITIES

One of the very important parts of countering InT is user activity monitoring (UAM). All of the best practices and mitigation strategies documents that were reviewed for this thesis included monitoring users on organizations' networks. As a high-level example, the Presidential Memorandum (Obama, 2012) directs agencies to include UAM in all InT programs.

UAM can be defined as a technological capability to monitor and capture actions and activities of individuals who access organizations' information systems in order to detect malicious insider activities (Larsen, 2014). Therefore, a UAM can be considered a tool that can collect, analyze, and alert technical indicators of InT. For effective user activity monitoring, this tool should be deployed on all networks and activities must be attributable to specific a user (Larsen, 2014).

According to Larsen (2014), the aim of UAM is to collect elaborative content about behavioral activities that can provide indications of InT. Therefore, the UAM tool should capture keystrokes, screen or full-screen video based on pre-defined triggering events such as specific sensitive keyword inputs, document actions (e.g., view, print, copy, and cut), search activities on the local computer or on the network, use of web browser, application usage (e.g., email, chat, and message), and use of removable media. With these capabilities, the UAM tool provides substantive data about employees' activities that no other type of tool can detect.

As mentioned before in this study, system administrators and privileged users pose special threats to organizations and they must be monitored closely with regard to organizations' computer systems. There are commercial-off-the-shelf products for user activity monitoring with similar capabilities. However, organizations should consider products that can provide additional monitoring capabilities for privileged user activities, such as changing permissions or ownership of files and objects, adding/deleting or other managerial actions on user and group accounts, and finally, changing configurations or security requirements for systems by using privileges.

The structure and deployment strategy of UAM may vary according to organizational needs. However, monitoring and recording everything on computer systems is neither practical nor possible. For successful user activity monitoring, organizations should have effective approaches to perform close monitoring and well-defined technical indicators that uniquely address who has the most access to the "crown jewels" of the organization or "the most to gain from obtaining access to" those jewels (Raytheon, 2009, p. 4).

B. PRACTICE #7 – PREVENT DATA EXFILTRATION

A malicious insider has many ways to compromise the information of an organization. Increasing information sharing capabilities on information systems not only makes it easier to transfer data within or out of an organization for business and other purposes, but also makes it more challenging to counter malicious insiders.

Even though organizations have specific data transfer procedures, employees with malicious intent can exfiltrate data via email, USB, or similar removable media (e.g., external hard drives, mobile devices, CDs, DVDs), cloud based storage, and printers (Silowash et al., 2012). Organizations must monitor and restrict access to these services and must account for all devices that connect to its computer systems (Silowash et al., 2012). For this reason, organizations should have data loss prevention (DLP) solutions for filtering data where data leaves the organization and respond properly when needed.

Gartner analysts Reed and Wynne (2016) define DLP as "technologies that, as a core function, perform both content inspection and contextual analysis of data at rest on-premises or in cloud applications and cloud storage, in motion over the network, or in use on a managed endpoint device" (p. 1). In fact, DLP emerged at the beginning of the 2000s for preventing organizations from unintentional or accidental data leakage out of their boundaries. Bekker (2015) states that after a series of insider incidents in both the public and private sector since 2010, DLP has gained its popularity again with additional capabilities to prevent intentional data theft by InT. Bekker also provides brief DLP architectures, which are very useful for gaining a better understanding of data loss prevention.

Architecturally, DLP can be divided into two main categories: endpoint or host-based DLP and network-based DLP. The former are typically agents that reside on endpoint devices, such as workstations, personal computers, databases, and servers, and monitor activity for potential violations. Agent-based DLP tools can also typically manage and monitor removable devices, such as USB drives, DVDs, etc., by controlling what data can be written to them, requiring encryption, etc. Network-based DLP tools monitor outbound traffic at common network egress points (typically via network TAPs [test access point] or SPAN [switch port analyzer] ports) and across common protocols and traffic such as Web/HTTP(S), email/SMTP, or file transfers/FTP. These tools look for data that might be deemed too sensitive to leave the corporate confines, then take some of the remediation actions outlined earlier. As is typically the case with information security, each approach has its advantages and limitations, and thus most DLP vendors now offer a combination of both endpoint and network-based DLP (Bekker, 2015).

According to Reed and Wynne (2016), DLP solutions not only prevent loss of data on endpoints, storage, or network but also help organizations by incorporating detection technologies to discover classified information within organizations. In essence, for mitigation of InT, organizations need DLP solutions to discover where their critical information resides and how to stop it going where it is not supposed to go via email, removable media, or cloud base storage.

C. PRACTICE #8 – USE SECURITY INFORMATION AND EVENT MANAGEMENT TECHNOLOGY

Organizations are using numerous security solutions to monitor, audit, and respond to their employee’s actions for protecting their systems. With other logging capabilities, these solutions log voluminous actions and events. Considering the number of logging nodes, employees, and different kinds of security solutions, overload of log data inevitably becomes challenging.

Even if it would be possible to handle that much data, it is not sufficient to prevent incidents by only logging all online and offline events. To extract useful information for decision making and more relevant alerts about malicious actions, log data must be correlated within its log source and with other multiple sources (Silowash et al., 2012). As Johnson, Takacs, and Hadley (2009) state, logs do not have value if they are not reviewed regularly or randomly.

The volume and complexity of the log data from security solutions requires organizations to select data sources. Organizations should decide which of these data feeds are critical for aggregation and correlation. CERT researchers think that, at minimum, the following types of events should be collected and correlated. Since this list is not broad enough for preventing and detecting every insider incident type, organizations should add other data feeds that are critical for their system:

- firewall logs
- unsuccessful login attempts
- intrusion detection systems
- intrusion prevention system logs
- web proxies
- antivirus alerts
- change management (Silowash et al., 2012, p. 56)

Security information and event management (SIEM) tools help organizations to collect log data from numerous nodes centrally and analyze them for anomaly detection (Callahan, 2013). SIEM technology enables analysts to view and query multiple log sources and correlate events with a single interface. Analysts Kavanagh and Rochford (2015) define SIEM as “security analytics to event data in real time for the early detection of targeted attacks and data breaches, and to collect, store, analyze and report on log data for incident response, forensics and regulatory compliance”(p. 1).

There are some important points that must be taken into account regarding the SIEM system. Firstly, SIEM must detect and alarm for anomalous actions that an everyday user does not do, such as installing a program or disabling a security feature. Secondly, different security solutions create logs in different formats. For correlation of events, these log formats must be normalized. Otherwise, useful information cannot be extracted with other than poor correlation. Finally, depending on the organizations' size someone should monitor the SIEM system regularly (Silowash et al., 2012).

Nearly all InT best practices or mitigation strategies in terms of technical controls suggest using a log correlation engine or SIEM tool. Therefore, organizations should use this technology without hesitation. Numerous SIEM products with different capabilities are available commercially. For successful selection, organizations should consider their size, as well as current and future security solutions in their criteria.

D. PRACTICE #9 – ESTABLISH A DEDICATED HUB FOR INSIDER THREATS

The critical importance of technical controls against insiders has been highlighted in the previous section. However, it is clear that organizations need a hub structure to gather and integrate technical and non-technical observables, do analysis and correlation of this gathered information, and apply appropriate handling of the indicators that cross thresholds.

To fulfill this need, the U.S. Department of Navy (DON) released an instruction for its InT program in October 2015 and directed establishment of an InT hub. In this instruction, the three primary functions of insider hub are listed as follows:

- Gather and integrate information from various sources
- Analyze that information to identify indications of possible malicious insider activity
- Ensure that Navy responds appropriately to all insider threat indicators (DON, 2015, p .13)

According to DON instruction (2015), the insider hub will be operated by InT personnel that include analysts and managerial staff. These personnel "require additional specialized insider threat training due to performance of functions and or duties within an insider threat program, or assigned to an activity that directly supports an insider threat mission" (DON, 2015, p. 14).

The insider hub must be provided with not only technical observables (indicators) but also non-technical observables and other information for effectively countering InT. To do that, DON directs that InT personnel have electronic access to security, counterintelligence, information assurance, human resources, and other means of information sources to identify, analyze, and respond to insider threat incidents (DON, 2015).

A hub-like structure is also recommended by other studies under different names. For example, Guido and Brooks (2013) recommend having a "Security Operations Center" that will perform most of the InT operations. Natural members of "Security Operations Center" and their functions are provided by Guido and Brooks in Table 7.

Table 7. Roles for Insider Threat Program. Source: Guido and Brooks (2013, p. 1835)

Name	Role	Function
Computer Network Defense Administrator	Deploys and operates auditing and preventative data sources.	Responsibilities are to deploy and maintain the sensor grid. Would likely be used during incident remediation. Has permission to make changes to enclaves and systems that they are responsible for.
Insider Threat Analyst	Performs technical analysis of the data to assess for any escalation.	Typically these are tiered subject matter experts at interpreting information from organizational auditing sources that could be indicative of a problem.
Insider Threat Engineer	Architects and engineers advanced technical capabilities for pursuing the malicious insider.	Engineers with subject matter expertise in insider threat prevention, auditing, correlation, large data sets and databases, and building complex automation systems.
LE/CI Agent	Government agent who is chartered and empowered to enforce law.	Typically leads the counterintelligence, espionage, or misuse investigation. May not be a technical role.

In fact, other DOD components have hub-like structures for InT and as stated in DON instruction (2015) their ultimate connection point will be the DITMAC, which will be the central hub "to understand and share information on the InT risk" (DITMAC, n.d.).

The Naval Postgraduate School has been tasked to assist the Navy Insider Threat Office in defining the organization and work flow for a conceptual InT hub (Figure 6). The current version of this conceptual model is the basis for the model in this thesis.

Inputs of this model are the data gathered from cyber controls (UAM, SIEM, DLP, network monitoring, etc.) and other data such as criminal history, polygraph results, and foreign travel records, which are important to identify InT in near-real time. These data are integrated and analyzed by analysts to get better informative data. Since one of the important pieces of countering InT is having possible indicators for different situations, the integrated and analyzed data are also used for developing new contexts to detect insider activities. Hub personnel utilize the organization's policy, previously extracted typical UAM behaviors and pre-defined threshold levels for analysis and context development activities.

Based on the threshold levels, analyzed data are separated into two databases. The triggering activities that raise flags are forwarded to "Flagged Data Distribution Database," and the activities that are accepted as normal are forwarded to "Un-flagged Data Repository." Suspicious activities in the flagged data database undergo a case management determination by an analyst or a senior analyst or hub manager. Based on the actual case, related CI, LE, security or other specialists are included for further specialized analysis.

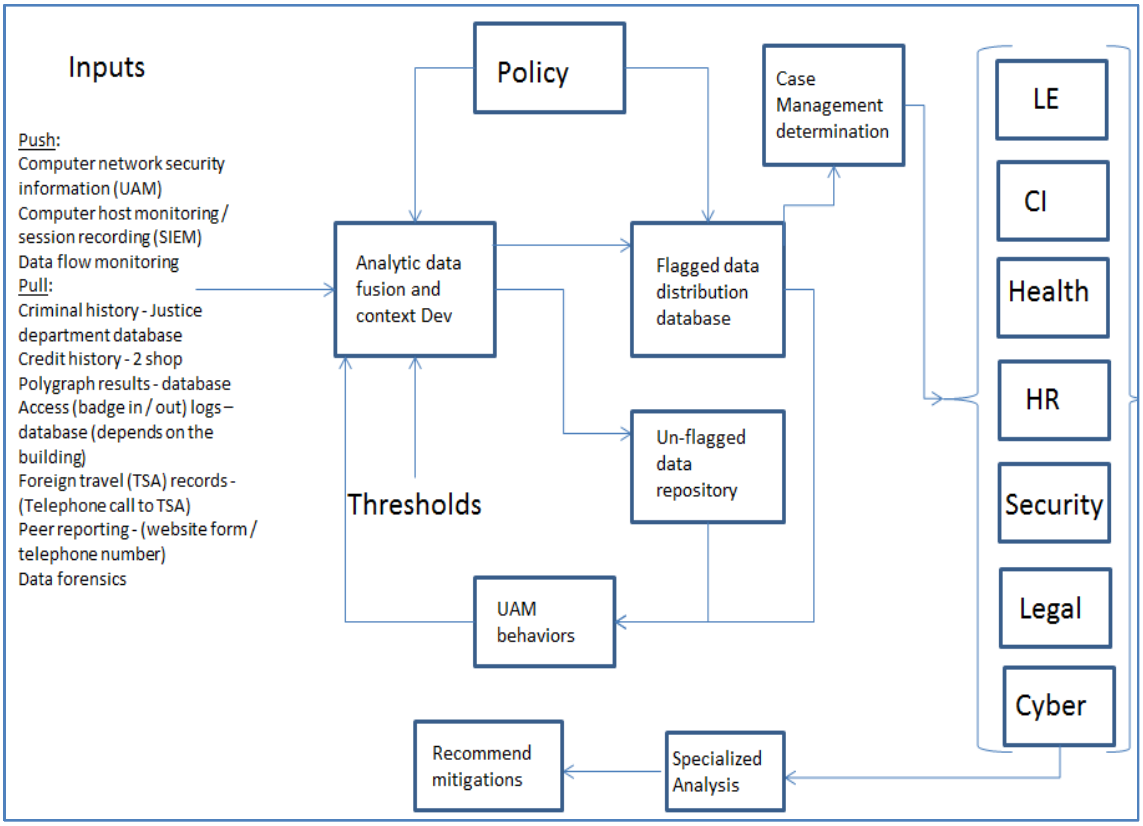

Inputs
Push:
Computer network security information (UAM)
Computer host monitoring / session recording (SIEM)
Data flow monitoring
Pull:
Criminal history - Justice department database
Credit history - 2 shop
Polygraph results - database
Access (badge in / out) logs – database (depends on the building)
Foreign travel (TSA) records - (Telephone call to TSA)
Peer reporting - (website form / telephone number)
Data forensics
Policy
Case Management determination
LE
CI
Health
HR
Security
Legal
Cyber
Analytic data fusion and context Dev
Flagged data distribution database
Un-flagged data repository
Thresholds
UAM behaviors
Recommend mitigations
Specialized Analysis

Figure 6. Conceptual Hub Structure for DON. Source: Gallup (2016).

In this phase, all information about employees gathered from technical controls and other sources are inspected closely. If the senior analyst and related specialists decide that detected indicators are at a concern level that an employee is or may be an InT, the senior officer or program manager of the InT program is notified by the hub manager. Upon reviewing indicators, the senior officer or program manager determines whether to initiate an inquiry or require closer and continuous monitoring of the employee.

There are some other important aspects of the model. For example, human resources, law enforcement, counterintelligence, and other specialists in the hub also recommend mitigations for the threats that they find. In addition, flagged data and un-flagged data repositories should be used regularly in order to extract patterns for detecting concerning behaviors and indicators via UAM.

Since this is a conceptual model, the number of managers, analysts, specialists and technical personnel (network administrator, database administrator, computer system engineer) may vary according to organization size. Finally, the functions and operations in this hub structure are explained at very high level although there are some important issues, such as how to decide credible indicators, how to establish effective communication inside the hub, and how to handle inquires.

E. EFFECTS OF TURKISH CULTURE ON IMPLEMENTATION OF TECHNICAL CONTROLS AND INSIDER HUB

According to Kedia and Bhagat (1988), the effectiveness of TOT (Transfer of Technology) depends on the characteristics of the technology. They continue their argument by stating that in recent years nearly all technology transfers involve product, process, and person-embodied characteristics. Considering the TOT model, even though the technical countermeasures presented in this study include process and person-embodied characteristics, these technical capabilities have product-embodied characteristic in general. In product-embodied technology transfer, one transfers physical products such as sophisticated computer components (Kedia & Bhagat, 1988).

Kedia and Bhagat (1988) argue that product-embodied technologies can be considered easier to transfer compared to others. They explain that cultural and management factors have a larger effect on process and person-embodied technology transfers. In this regard, it can be said that the effects of Turkish culture would be limited on implementation of technical countermeasures. Still, some important points exist as follows.

Having a high uncertainty avoidance characteristic, Turkish organizations tend to have more rules and regulations. This characteristic can lead to exhaustive monitoring of user movements, recording data transfers, and logging all actions on an organization's computer system. Without considering legal issues, having too many rules and monitoring more than necessary actions would lead to false positives detecting insider activities and could cause missing actual InT. More importantly, efforts to integrate every possible data source, including excessive user monitoring, into analysis would eventually overwhelm the insider hub and make it ineffective.

According to Hofstede et al. (2010), in a high PDI scoring culture superiors and managers can have a tendency to feel existentially unequal. They feel lower ranking employees in the organization are inferior to themselves, and this mindset will eventually cause resistance to the monitoring of their activities by subordinates. They would ask for privileges to refrain from being monitored, which can cause pressure over hub personnel.

As stated before in this study, employees in collectivist countries see the workplace as an in-group in which family-like relationships develop. Since the personal relationships come before the tasks in collectivist societies, these relationships should be established prior to performing tasks (Hofstede et al., 2010). As a result, the selection of insider hub personnel becomes important for Turkish organizations, which have a collectivist nature. Selecting the best analysts and technicians for the hub does not necessarily mean that they will work in harmony. These hub members should not have conflicts between each other because, unlike the employees in individualist societies, these personnel could focus on conflicts instead of tasks.

Positively, the high uncertainty avoidance characteristic of Turkish culture can ease implementation of technical controls. According to Hofstede et al. (2010), high uncertainty avoidance societies are better on implementation instead of innovation, and they have a belief in experts and technical solutions. Thus, a new technical solution and dedicated insider hub would be accepted as a cure to insider activities. In addition, talented experts and technicians would be assigned to perform the tasks in the insider hub for fast and flawless implementation of this new technology.

Technical countermeasures against InT require monitoring and capturing user data. These are very important tasks for countering insiders, and they are not straightforward. National cultures have an influence on defining sensitive data and deciding which user information to capture (Flynn et al., 2013).

THIS PAGE INTENTIONALLY LEFT BLANK

VI. RECOMMENDATIONS, FUTURE RESEARCH, AND CONCLUSIONS

Best practices to implement in TGCG for countering InT were presented in Chapter IV and Chapter V. Since implementing these practices can be accepted as a kind of technology transfer, the effects of Turkish culture on this transfer were analyzed by using Hofstede et al.'s (2010) study about cultural differences between nations. Based on the analysis, the final part of this thesis includes recommendations to TGCG for reducing the effects of cultural differences while implementing technical and non-technical countermeasures against InT, proposes an InT hub structure for TGCG, suggests future research areas, and ends with some final thoughts.

A. CONDUCTING INSIDER THREAT RISK ANALYSIS IN TGCG

Because of their collectivist mindset, the employees that conduct risk assessment in TGCG would see the entire organization as a family and would possibly believe the probability of being attacked by their own friends is very low, which will decrease the effectiveness of risk assessment. For this reason, TGCG should get professional assistance while conducting risk assessment. Needless to say, non-disclosure agreements between a consulting company and TGCG about organizational information must be very strict. Another option for having an outsider's eye could be including other armed forces' security personnel in the risk assessment process.

Because of high the uncertainty avoidance characteristic of Turkish culture, the service periods of employees in TGCG are usually more than 15 years, and in this period they are assigned to various positions in the organization. This situation increases the probability of conveying previous positions' information and access rights to the new one. Risk assessors must review present plans and procedures to see whether they include limitation of previous electronic or physical access rights when assigned to a new position. If these procedures do not include this limitation or they are ambiguous, the risk assessors must include this in their final report.

As another consequence of high uncertainty avoidance, Turkish culture would lead TGCG members to have an instinctive trust in existing technical specialists, system administrators, and technological solutions in TGCG, which would harm risk assessment. Thus, the real capacity and usability of existing technologies must be assessed carefully. The vulnerabilities of existing systems against InT must be tested. An example of this can be an insider penetration test via a trusted penetration test company. The results of this test can also be useful for implementation and adaptation of other technologies, such as UAM, DLP and SIEM.

In addition, system administrators' and other privileged users' access rights must be examined case by case. Since these kinds of examinations require high technical knowledge, it will also require professional assistance. TGCG can use other forces' IT professionals or can sign a contract with an accredited company.

B. CREATING INSIDER THREAT POLICIES AND PROCEDURES FOR TGCG

While defining policies and procedures, TCGC should consider at a minimum the issues that were explained in Chapter IV. The following recommendations would be helpful when applying these issues to TGCG.

The contribution of subordinates, who have great tacit knowledge about their organization, to policy and procedure creation processes would be limited because of the power distance gap in the workplace, where subordinates are prone to believe that only the superiors have authority and knowledge for any policy and procedure creation. TCGC should involve as much as possible the contribution of its employees who are experienced in their respective areas. This would lead to having much more sound policies and procedures.

As another effect of high power distance in workplace, superiors are likely to ask for more privileges and access rights more than they need because they feel they are existentially superior. Policy and procedure creators should set privileged users' access rights according to the "need to know" principle, and these users should not be given more access rights than needed.

Policies and procedures created for TGCG to counter InT should not be overly detailed and excessive because of the high uncertainty avoidance characteristic. Policy makers should create concise and coherent policies and procedures to avoid drowning employees in details.

Finally, to overcome the difficulties of being a high-context culture, TGCG should not expect its cultural context to fill the gaps when communicating the newly created policies and procedures. TGCG should communicate these policies explicitly and clearly for the purpose of preventing misunderstandings and unintended harm to internal systems.

C. DEVELOPING AN INSIDER THREAT PROGRAM FOR TGCG

The required topics for an InT program have already been stated in Chapter IV. Establishing an InT team in TGCG to execute the program would not be hard because of the high power distance nature of organization. However, in order to increase the contribution of lower ranking employees to the program, TGCG still needs to decrease any unwanted effects of high PDI. To do that, TGCG should delegate more responsibility to lower ranking employees, should consider their opinion in decision-making mechanisms, and should appreciate their contributions to the InT program.

As recommended in the risk assessment section, TGCG should also get professional help from outside of the organization to establish an InT program because of the same considerations regarding being a collectivist society. Otherwise, collectivist effects of family-like relationships and the need for establishing links between team members before organizing an insider team would harm the effectiveness of InT program.

In addition, having a legal consultant from outside of the TGCG or using its own lawyers and legal advisers would be beneficial to establish a legitimate InT program and to eliminate duplicative or excessive rules or regulations that can result from the high uncertainty avoidance characteristic of the Turkish culture.

D. PROVIDING INSIDER THREAT AWARENESS TRAININGS IN TGCG

The instructors of InT awareness training programs in TGCG should themselves get longer and more detailed training before they start giving training sessions to other employees. Training and education is instructor centered in high PDI societies like Turkey. Because of this cultural dimension, employees expect to obtain deep knowledge from their instructors and their contribution to the training would be limited. As another reflection of the same dimension, the presence of superiors in lectures as attendees or lecturers would emphasize the importance of the InT issue in TGCG.

In a collectivist society, in general, the goal of education is to learn how to do something instead of to understand how to learn (Hofstede et al., 2010). The goal of learning how to do something would require more formal training sessions and continuous learning within the TGCG. Once or twice a year formal awareness training with limited hours would not be sufficient for such an important topic. TGCG should provide awareness raising opportunities throughout the year by using banners in computer systems, posters, and short presentations that are held in departments individually.

Since employees tend to think of their co-workers as family members in collectivist societies, they can feel that reporting their friends is some kind of betrayal to the family. It should be emphasized in all security and InT awareness training that any employees showing dangerous behaviors must be reported before they harm the entire TGCG family. In addition, TGCG should train its employees how to report secretly and assure that reporting employees will remain anonymous against possible pressure from other employees.

E. REVIEWING EMPLOYEE TERMINATION PROCEDURES OF TGCG

TGCG is a military organization and already has strict employee termination procedures. Departed employees cannot access computer systems and physical facilities upon termination. However, risks remain because of cultural effects.

As stated in Chapter IV, termination of an employee because of violation of rules causes feelings of shame on the part of the departing employee in collectivist societies.

Even though it has very strict rules for employee termination, TGCG should refrain from fostering feelings of shame in a departing employee, particularly in front of other employees. Otherwise, this strong feeling can cause the shamed employee to launch an insider attack against TCGC after his or her termination.

Furthermore, such incidents may not occur in the form of sudden, single-handed attacks. As noted previously, employees in TGCG are likely to have long service periods and close relationships in the workplace because of the combined effects of high uncertainty avoidance and collectivism. Departed employees can try to use these strong, long-established relationships after being terminated to access TGCG facilities and information systems for insider activities. TGCG should notify all components with the name of any terminated employee. In addition, this notification should warn other employees about not disclosing any information and not allowing a terminated employee into TGCG facilities. To emphasize the importance of this vulnerability, it must be included in all formal insider awareness training and posters, banners, etc.

F. UTILIZING TECHNICAL CONTROLS IN TGCG

As explained in Chapter V, it is expected that the effects of cultural differences on technical controls would be less than the effects on non-technical controls. However, culture will be significantly important while implementing these new technologies. TGCG should consider the following recommendations to minimize cultural influences that might hinder success.

As an institution characterized by high uncertainty avoidance, TGCG is likely to overuse the technical controls available. User activity monitoring, network monitoring, data collection, integration and correlation activities might be performed excessively. TGCG should focus on protecting its "crown jewels" and defining better threshold levels to detect insider activities. Well-defined threshold levels not only would lessen the workload of the insider hub, but also would decrease the number of false positives.

Furthermore, the feeling of being monitored on TGCG computer systems and networks would lead to disgruntlement among superiors, privileged users, and system administrators. Those in high ranking positions may feel existentially superior because of the high power distance characteristic of the culture. These privileged users may request privileges for less monitoring and may try to use their power to put pressure on hub personnel from the very beginning of the InT program. To deal with this pressure, the insider hub organization should be under the direct control of very high-level management.

Clearly, the personnel selection process for the TGCG insider hub is very important, and it can be very challenging. TGCG should select personnel who can work in harmony with others in the hub. Conflicts between hub staff can lead to deterioration of in-group close relationships because of the collectivist nature of workplace. Conflicts must not be considered as casual problems between two individuals, and the hub manager should make efforts to solve these problems as soon as possible. Finally, following the high uncertainty avoidance characteristic, TGCG should assign talented technical experts for managing technical controls and operating the insider hub, which will facilitate fast and flawless implementation of new technical countermeasures against InT.

G. A PROPOSED INSIDER THREAT HUB ORGANIZATION FOR TGCG

It is clear that organizations need an insider hub. An example hub structure that is proposed for the U.S. Navy was explained in Chapter V. While accepting inevitable similarities, we are proposing a hub structure for TGCG as shown in Figure 7. In this figure, boxes represent entities and they are the source or destination of data. Curved boxes represent processes where tasks are performed. Cylinders represent databases where processed data are stored. Required personnel to carry out hub operations are presented in Appendix B.

The data about employees are collected via automated and semi-automated means as inputs of the hub. Input data include user activity monitoring records, network monitoring records, criminal history, personal reports, evaluation reports, access logs, peer reporting, foreign travels, data forensics, and financial status. Analysts perform integration and analysis of these data to extract valuable information. Analysts, basically, need two important things for their tasks: Tools and thresholds. There are commercial-off-the-shelf products for data integration, correlation, and analysis that can be used in the hub. TGCG should make an assessment and decide which are the most useful products to buy for its needs. Setting thresholds is much harder to achieve. Thresholds are very important to work effectively. Because of its high uncertainty avoidance, TGCG should be very careful about setting thresholds. Efforts to catch every bit of very high fidelity information via computer systems would likely cause dysfunction within the insider hub.

Let us consider the work flow within the hub after thresholds are established. User activities that meet thresholds trigger flags and are recorded to a “Flagged Data” database. Before determination of a case management type by the hub manger, these suspicious activities are reviewed by the senior analyst. The senior analyst can change the status of the flag if he is not satisfied with the detected activity. When the senior analyst approves the status of a flag-raising insider activity, he forwards it to the hub manager for case management determination.

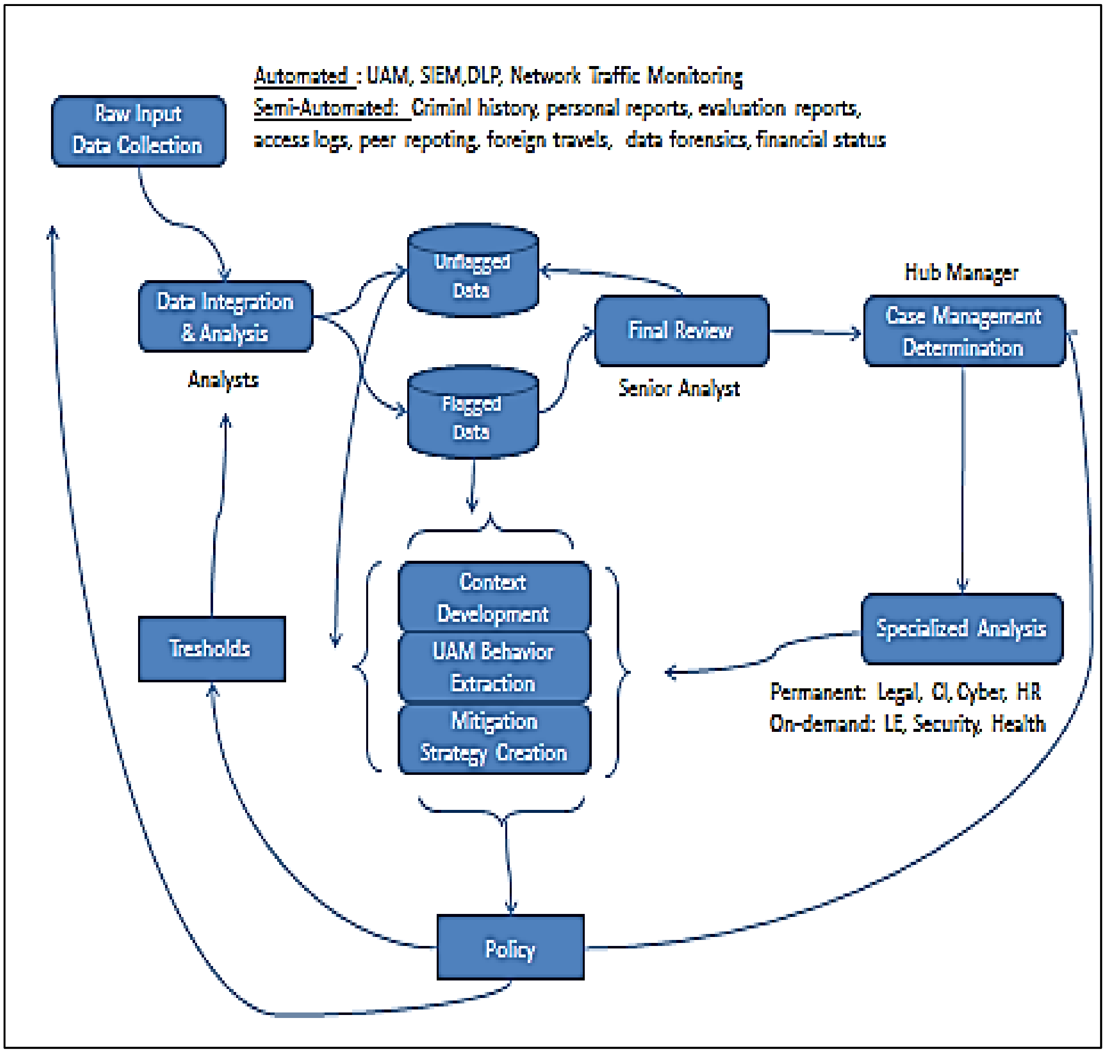

Automated : UAM, SIEM,DLP, Network Traffic Monitoring
Semi-Automated: Criminl history, personal reports, evaluation reports, access logs, peer repoting, foreign travels, data forensics, financial status
Raw Input Data Collection
Data Integration & Analysis
Analysts
Unflagged Data
Flagged Data
Final Review
Senior Analyst
Hub Manager
Case Management Determination
Context Development
UAM Behavior Extraction
Mitigation Strategy Creation
Tresholds
Specialized Analysis
Permanent: Legal, CI, Cyber, HR
On-demand: LE, Security, Health
Policy

Figure 7. Proposed Hub Structure for TGCG.

The hub manager decides which specialized analysts will examine the case. Legal, counterintelligence, cyber, and human resources specialists are permanent members of the hub. If the hub manager needs law enforcement, security, health, or other specialists, he contacts them as soon as possible. These on-demand specialists must be pre-selected and the hub manager should not have any ambiguity when he needs them. Results of specialized analysis can produce close monitoring of a possible insider or induce taking proper actions immediately, such as prohibiting the insider's activity in computer systems, banning the insider from entering facilities, or starting an inquiry about the suspected insider.

Flagged and unflagged data repositories and specialized analysis results are used for new context developments, new UAM behavior extractions and creation of mitigation strategies. TGCG should use these developments, which can be named as lessons learned, in order to improve InT policies. This has prime importance because policy affects what data to capture, what threshold level to set, and how to determine the case management type.

H. FUTURE WORK

This thesis examined research and resources about InT risk mitigation techniques and identified the best practices vital for TGCG. Implementation of these best practices is analyzed by only one of the moderating factors of technology transfer from Kedia and Bhagat's (1988) study, which is "societal culture-based differences."

The other moderating factor of technology transfer in the Kedia and Bhagat study, "absorptive capacity of recipient organization," was not a focus of this thesis. However, in addition to understanding the effects of national cultural differences, it is important to identify the recipient organization's specific factors, such as local or cosmopolitan orientation of organization, the level of sophisticated technology in the organization, or current management processes of the organization. Thus, future research could target the absorptive capacity of TGCG in terms of implementing international counter-insider threat best practices.

Another further study based on this research could focus on extracting Turkish-specific or organization-specific insider threat indicators from insider incidents. In fact, this step comes after one important issue, which is establishing an InT database in Turkey, and could be the subject of another study. Addressing the need for an InT database, further study should consider issues such as how to get data about insider incidents form public and private organizations, defining the classification level of data in the database, deciding how much of data can be disclosed to public, specifying the techniques for analysis of data, etc. After the establishment of the InT database, the future analysis could be done for extracting data concerning behaviors and InT indicators.

I. LAST WORDS

Like many other information security topics, there is much ongoing research about insider threats. Most of the research originates from U.S. public and private organizations and applying the findings of these studies to other countries involves technology transfer challenges. There are only a handful of research studies that include cross-cultural effects of implementing this technology to other countries.

Adapting a technology, which includes people, procedures, and products, from another country is not straightforward and has the potential to fail or be ineffective because of cultural differences. Buying a computer program or applying a practice that works well in an organization does not mean it will work in another organization that resides in completely different cultural context. Understanding these cultural differences and taking them into account before implementing a new technology would increase the probability of successful technology transference.

APPENDIX A. MAPPING OF BEST PRACTICES

The provided best practice resources should not be considered as stand-alone documents. Mostly, these resources review multiple InT publications, add their experiences, and include their insights in order to provide better InT risk mitigation techniques. To illustrate, the Intelligence and National Security Alliance's InT roadmap reviews more than 200 publications before providing 13 essential elements for an InT program.

The coding for informative resources is as follows:

Common Sense Guide to Mitigating Insider Threats (4th ed.) by Silowash et al. (2013). → ***CSG Best Practice***

"Best Practices against Insider Threats in All Nations" by Flynn et al. (2013) → ***AllNations Best Practice***

"The CERT Top 10 List for Winning the Battle against Insider Threats" by Cappelli (2012). → ***CERT Top10***

"Insider Threats: DOD Should Strengthen Management and Guidance to Protect Classified Information and Systems" (GAO-15-544) by Kirschbaum and Wilshusen (2015). → **GAO Framework**

National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs by Obama (2012). → **NITP Standards**

"Best Practices for Mitigating and Investigating Insider Threats" by Raytheon (2009). → ***RAY Best Practice***

"A Roadmap for Identifying and Countering Insider Threats in the Private Sector by Intelligence and National Security Alliance" (n.d.). → **INSA Roadmap**

"Insider Threats Best Practices Guide by SIFMA." (2014). → **SIFMA Best Practice**

Practice	Informative References
Best Practice #1 Conduct Enterprise-Wide Risk Assessment	CSG Best Practice #1 AllNations Best Practice #1 CERT Top10 #9 GAO Framework – Prevent/4 RAY Best Practice #1 INSA Roadmap #4 SIFMA Best Practice – ID.RA
Best Practice #2 Define Policies and Procedures, Enforce Consistently	CSG Best Practice #2 AllNations Best Practice #2 CERT Top10 #7 GAO Framework – Deter/2 RAY Best Practice #7 INSA Roadmap #6 SIFMA Best Practice – PR.IP
Best Practice #3 Develop A Formalized Insider Threat Program	CSG Best Practice #16 AllNations Best Practice #16 CERT Top10 #1 GAO Framework – Deter/1 NITP Standards – Section D. INSA Roadmap #1 SIFMA Best Practice – ID.GV
Best Practice #4 Provide Insider Threat Awareness Training	CSG Best Practice #3 AllNations Best Practice #3 CERT Top10 #5 GAO Framework – Prevent/2 NITP Standards – Section F INSA Roadmap #7 SIFMA Best Practice – PR.AT
Best Practice #5 Review Employee Termination Processes	CSG Best Practice #14 AllNations Best Practice #14 CERT Top10 #4 GAO Framework – Take Action/2 SIFMA Best Practice – PR.AC

Best Practice #6 Monitor User Activities	CSG Best Practice #10 AllNations Best Practice #10 CERT Top10 #8 GAO Framework – Detect/2 NITP Standards – Section F RAY Best Practice #4&5 INSA Roadmap #9 SIFMA Best Practice – DE.AE/DE.CM
Best Practice #7 Prevent Data Exfiltration	CSG Best Practice #19 AllNations Best Practice #19 CERT Top10 #8 GAO Framework – Prevent/3 NITP Standards – Section H INSA Roadmap #9 SIFMA Best Practice – DE.AE
Best Practice #8 Use Security Information and Event Management Technology	CSG Best Practice #12 AllNations Best Practice #12 CERT Top10 #8 GAO Framework – Prevent/5 NITP Standards – Section E INSA Roadmap #9&10 SIFMA Best Practice – DE.AE
Best Practice #9 Establish A Dedicated Hub for Insider Threats	CSG Best Practice #16 AllNations Best Practice #16 CERT Top10 #1 GAO Framework – Prevent/1 NITP Standards – Section E&F INSA Roadmap #2 SIFMA Best Practice – ID.GV

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B. REQUIRED PERSONNEL FOR AN INSIDER HUB IN THE TURKISH GENDARMERIE

Role	Required Number	Comments
Hub Manager	1	
Information System Engineer	2	Responsible for engineering technical controls on TGCG’s information systems. At least one of them is trained for UAM system engineering.
Database Administrator	2	At least one of them is trained for UAM database.
Network Administrator	1	
Senior Analyst	1	
General Analyst	3	
Legal Specialist	1	
Cyber Specialist	1	
Counterintelligence Specialist	1	
Human Resources Specialist	1	
Law Enforcement Specialist	1	On-demand
Security Specialist	1	On-demand
Health Specialist	1	On-demand

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

A roadmap for identifying and countering insider threats in the private sector. (n.d.). [Online]. Retrieved from http://www.insaonline.org/InsiderThreat

Appelbaum, S. H. (1997). Socio-technical systems theory: An intervention strategy for organizational development. *Management Decision*, *35*(6), 452–463. doi:10.1108/00251749710173823

Band, S. R., Cappelli, D. M., Fischer, L. F., Moore, A. P., Shaw, E. D., & Trzeciak, R. F. (2006). Comparing insider IT sabotage and espionage: A model-based analysis (No. CMU/SEI-2006-TR-026). *Carnegie-Mellon Univ. Pittsburgh, PA Software Engineering Inst.* Retrieved from http://oai.dtic.mil/oai/oai?verb=getRecord&metadata Prefix=html&identifier=ADA459911

Baxter, G., & Sommerville, I. (2011). Socio-technical systems: From design methods to systems engineering. *Interacting with Computers*, *23*(1), 4–17.doi: 10.1016/ j.intcom.2010.07.003

Bekker, G. (2015). The data loss prevention market by the numbers: 2014–2019. *451 Research*. Retrieved from https://digitalguardian.com/blog/data-loss-prevention-market-numbers-451-research-report

Bishop, M., Engle, S., Frincke, D. A., Gates, C., Greitzer, F. L., Peisert, S., & Whalen, S. (2010). A risk management approach to the "insider threat." *Insider Threats in Cyber Security* (pp. 115–137). doi: 10.1007/978-1-4419-7133-3_6

Bostrom, R. P., & Heinen, J. S. (1977). MIS problems and failures: A socio-technical perspective, part II: The application of socio-technical theory. *MIS Quarterly*, *1*(4), 11–28. doi:10.2307/249019

Bozeman, B. (2000). Technology transfer and public policy: A review of research and theory. *Research Policy*, *29*(4), 627–655. doi: 10.1016/S0048-7333(99)00093-1

Callahan, C. J. (2013). *Security information and event management tools and insider threat detection* (Master's thesis). Retrieved from http://oai.dtic.mil/oai/oai? verb=getRecord&metadataPrefix=html&identifier=ADA589914

Cappelli, D. (2012, February). The CERT top 10 list for winning the battle against insider threats. Presented at RSA Conference, San Francisco, CA. Retrieved from https://www.rsaconference.com/writable/presentations/file_upload/star-203.pdf

Cappelli, D. M., Moore, A. P., & Trzeciak, R. F. (2012). *The CERT guide to insider threats: How to prevent, detect, and respond to information technology crimes (theft, sabotage, fraud).* Westford, MA: Addison-Wesley.

Cartelli, A. (2007). Socio-technical theory and knowledge construction: Towards new pedagogical paradigms. *Issues in Informing Science and Information Technology*, *4*(27), 1–14. Retrieved from http://proceedings.informingscience. org/I nSITE2007/IISITv4p001-014Cart339.pdf

Caruso, V. L. (2003). *Outsourcing information technology and the insider threat* (Master's thesis). Retrieved from http://dtic.mil/dtic/tr/fulltext/u2/ a415113.pdf

Cohen, W. M., & Levinthal, D. A. (1990). Absorptive capacity: A new perspective on learning and innovation. *Administrative Science Quarterly*, 128–152. Retrieved from http://web.iaincirebon.ac.id/ebook/indrya/bandura/inovasi/Cohen LevinthalASQ.pdf

Costa, D. L., Collins, M. L., Perl, S. J., Albrethsen, M. J., Silowash, G. J., & Spooner, D. L. (2014). An ontology for insider threat indicators development and applications. *Carnegie-Mellon Univ. Pittsburgh, PA Software Engineering Inst.* Retrieved from http: //oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix= html&identifier= ADA615757

Dedman, B., Brunker, M., & Cole, M. (2014, May 26). Who is Edward Snowden, the man who spilled the NSA's secrets? *NBC News*. Retrieved from http://www. nbcnews. com/feature/edward-snowden-interview/who-edward-snowden-man-who-spilled-nsas-secrets-n114861

Department of Defense (U.S.). (2014, Sep. 30). *DOD insider threat program* (DOD Directive 5205.16). Washington, DC: Work, R. O. Retrieved from http://www.dtic.mil/whs/ directives/corres/pdf/520516p.pdf

Department of the Navy (U.S.). (2015, Oct. 1). *Navy Insider Threat Program* (OPNAV Instruction 5510.165.A.). Washington, DC: Braun, R.R. Retrieved from https://fas.org/irp/DODdir/navy/opnavinst/ 5510_165a.pdf

DOD Insider Threat Management Analysis Center (DITMAC). (n.d.). Retrieved from http://www.dss.mil/about_dss/ditmac.html#1

Exec. Order No. 13587. (2011). 3 C.F.R. 13587: *Structural reforms to improve the security of classified networks and the responsible sharing and safeguarding of classified information.* Retrieved from https://www.gpo.gov/fdsys/pkg/FR-2011-10-13/pdf/2011-26729.pdf

Flynn, L., Huth, C., Trzeciak, R., & Buttles, P. (2013). Best practices against insider threats for all nations. In *2012 Third Worldwide Cybersecurity Summit (WCS)* (pp. 1–8). IEEE. doi: 10.1109/WCS.2012.6780874

Gallup, S.P. (2016). [Navy insider threat to cyber-security research project]. Unpublished raw data.

Glenn, E. S., & Glenn, C. G. (1981). *Man and mankind: Conflict and communication between cultures*. Norwood, NJ: Ablex.

Greitzer, F. L., & Frincke, D. A. (2010). Combining traditional cyber security audit data with psychosocial data: Towards predictive modeling for insider threat mitigation. *Insider Threats in Cyber Security* (pp. 85–113). doi:10.1007/978-1-4419-7133-3_5

Guido, M. D., & Brooks, M. W. (2013). Insider threat program best practices. In *System Sciences (HICSS), 2013 46th Hawaii International Conference on* (pp. 1831–1839). IEEE. doi: 10.1109/HICSS.2013.279

Hagel, C. (2014). Final recommendations of the Washington Navy Yard shooting internal and independent reviews [Memorandum]. Washington, DC: Secretary of Defense. Retrieved from https://fas.org/sgp/news/2014/03/secdef-rec.pdf

Hofstede, G. (1980). *Culture's consequences: Comparing values, behaviors, institutions and organizations across nations*. Beverly Hills, CA: Sage.

Hofstede, G. (1991). *Cultures and organizations: Software of the Mind* (1st ed.). Maidenhead, UK: McGraw-Hill.

Hofstede, G., Hofstede, G. J., & Minkov, M. (2010). *Cultures and organizations: Software of the Mind* (3rd ed.). New York, NY: McGraw-Hill.

Hunker, J., & Probst, C. W. (2011). Insiders and insider threats-an overview of definitions and mitigation techniques. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, *2*(1), 4–27. Retrieved from http://isyou.info/ jowua/papers/jowua-v2n1-1.pdf

Johnson, D. J., Takacs, N., & Hadley, J. (2009). Securing stored data. *Computer Security Handbook* (5th ed.) 36–1. Hoboken, NJ: John Wiley & Sons, Inc.

Kavangh, K.M., Rochford, O. (2015). Magic quadrant for security information and event management. *Gartner Group Research Note.* Retrieved from https://scadahacker.com/library/Documents/White_Papers/Gartner%20-%20Magic%20Quadrant%20for%20SIEM%20-%202015.pdf

Keating, C. B., Fernandez, A. A., Jacobs, D. A., & Kauffmann, P. (2001). A methodology for analysis of complex sociotechnical processes. *Business Process Management Journal*, *7*(1), 33–50. doi: 10.1108/14637150110383926

Kedia, B. L., & Bhagat, R. S. (1988). Cultural constraints on transfer of technology across nations: Implications for research in international and comparative management. *Academy of Management Review*, *13*(4), 559–571. doi: 10.5465/AMR.1988.4307424

Keeney, M., Kowalski, E., Cappelli, D., Moore, A., Shimeall, T., & Rogers, S. (2005). Insider threat study: Computer system sabotage in critical infrastructure sectors. *U.S. Secret Service and CERT Coordination Center/SEI*. Retrieved from http: //oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier= ADA441249

Kirschbaum, J.W., & Wilshusen, G.C. (2015). Insider threats: DOD should strengthen management and guidance to protect classified information and systems (GAO-15-544). Washington, DC: Government Accountability Office. Retrieved from www.gao.gov/assets/680/670570.pdf

Kowalski, E., Conway, T., Keverline, S., Williams, M., Cappelli, D., Willke, B., & Moore, A. (2008). Insider threat study: Illicit cyber activity in the government sector. *U.S. Department of Homeland Security, U.S. Secret Service, CERT, and the Software Engineering Institute (Carnegie Mellon University).* Retrieved from http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=52227

Kowalski, E., Cappelli, D., & Moore, A. (2008). Insider threat study: Illicit cyber activity in the information technology and telecomunication sectors. *U.S. Secret Service, CERT, and the Software Engineering Institute (Carnegie Mellon University).* Retrieved from http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=52227

Larsen, P. L. (2014). Clarification of enterprise audit management (EAM), user activity monitoring (UAM), continuous monitoring, and continuous evaluation [Memorandum]. Washington, DC: Office of the Co-Directors. Retrieved from https://www.ncsc.gov/nittf/docs/EAM_ UAM_ and_Continuous_Monitoring_ Definitions-Signed.pdf

Magklaras, G. B., & Furnell, S. M. (2001). Insider threat prediction tool: Evaluating the probability of IT misuse. *Computers & Security*, *21*(1), 62–73. doi:10.1016/ S0167-4048(02)00109-8

Nakata, C. (Ed.). (2009). *Beyond Hofstede: Culture frameworks for global marketing and management*. doi:10.1057/9780230240834

Nurse, J. R., Buckley, O., Legg, P. A., Goldsmith, M., Creese, S., Wright, G. R., & Whitty, M. (2014). Understanding insider threat: A framework for characterising attacks. *Security and Privacy Workshops* (pp. 214–228). doi:10.1109/SPW.2014.38

Obama, B. (2012). National insider threat policy and minimum standards for executive branch insider threat programs [Memorandum]. Washington, DC:White House. Retrieved from http://www.ncsc.gov/nittf/docs/National_Insider_Threat_Policy.pdf

Probst, C. W., Hunker, J., Gollmann, D., & Bishop, M. (2008). Countering insider threats. *Dagstuhl Seminar Proceedings*. Retrieved from http://drops.dagstuhl.de/opus/volltexte/2008/1793

Randazzo, M. R., Keeney, M., Kowalski, E., Cappelli, D., & Moore, A. (2004). Insider threat study: Illicit cyber activity in the banking and finance sector (No. CMU/SEI-2004-TR-021). *Carnegie-Mellon Univ. Pittsburgh, PA Software Engineering Inst*. Retrieved from http: //oai.dtic.mil/oai/oai?verb=getRecord &metadataPrefix=html& identifier= ADA441249

Raytheon. (2009) Best practices for mitigating and investigating insider threats [White paper]. *Raytheoncyber Resources.* Retrieved from http://www.raytheon.com/capabilities/ rtnwcm/groups/iis/documents/content/rtn_iis_whitepaper-investigati.pdf

Reed, B., & Wynne, N. (2016). Magic quadrant for enterprise data loss prevention. *Gartner Group Research Note.* Retrieved from https://info.digitalguardian.com/rs/768-OQW-145/images/2016-Gartner-Magic-Quadrant-for-Enterprise-Data-Loss-Prevention.pdf

Roessner, J. D. (2000). Technology transfer. *Science and Technology Policy in the U.S.. A Time of Change.* London: Longman.

Schultz, E. E. (2002). A framework for understanding and predicting insider attacks. *Computers & Security*, *21*(6), 526–531. doi:10.1016/S0167-4048(02)01009-X

SIFMA. (2014). Insider threat best practices guide (White paper). *SIFMA Cyber Security Resource Center*. Retrieved from http://www.sifma.org/uploadedfiles/issues/technology_and_operations/cyber_security/insider-threat-best-practices-guide.pdf?n=72596

Silowash, G., Cappelli, D., Moore, A., Trzeciak, R.., Shimeall, T., & Flynn, L. (2012). *Common Sense Guide to Mitigating Insider Threats, 4th Edition* (CMU/SEI-2012-TR-012). Retrieved from http://resources.sei.cmu.edu/asset_files/TechnicalReport/2012_005_001_34033.pdf

Tate, J. (2013, August 21). Bradley Manning sentenced to 35 years in wikileaks case. *The Washington Post*. Retrieved from https://www.washingtonpost.com/ world/national-security/judge-to-sentence-bradley-manning-today/2 013/08/20/85bee184-09d0-11e3-b87c-476db8ac34cd_story.html

Trist, E. L. & Bamford, K. W. (1951). Some social and psychological consequences of the longwall method of coal getting. *Human Relations, 4*(3), 3–38. doi: 10.1177/001872675100400101

Wood, B. (2000). An insider threat model for adversary simulation. *SRI International, Research on Mitigating the Insider Threat to Information Systems, 2*, 1–3. Retrieved from http://oai.dtic.mil/oai/oai?verb=getRecord&metadata Prefix= htm

Zahra, S. A., & George, G. (2002). Absorptive capacity: A review, reconceptualization, and extension. *Academy of Management Review*, *27*(2), 185–203. Retrieved from http://amr.aom.org/content/27/2/185.full.pdf+htmll&identifier=ADA386077

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California